The Statistical Physics of Regular Low-Density Parity-Check Error-Correcting Codes

Tatsuto Murayama[1],Yoshiyuki Kabashima[1], David Saad[2] and Renato Vicente[2]

[1] *Department of Computational Intelligence and Systems Science, Tokyo Institute of Technology, Yokohama 2268502, Japan.*

[2] *The Neural Computing Research Group, Aston University, Birmingham B4 7ET, UK.*

Abstract

A variation of Gallager error-correcting codes is investigated using statistical mechanics. In codes of this type, a given message is encoded into a codeword which comprises Boolean sums of message bits selected by two randomly constructed sparse matrices. The similarity of these codes to Ising spin systems with random interaction makes it possible to assess their typical performance by analytical methods developed in the study of disordered systems. The typical case solutions obtained via the replica method are consistent with those obtained in simulations using belief propagation (BP) decoding. We discuss the practical implications of the results obtained and suggest a computationally efficient construction for one of the more practical configurations.

I. INTRODUCTION

Error-correcting codes are commonly used for reliable data transmission through noisy media, especially in the case of memoryless communication where corrupted messages cannot be repeatedly sent. These techniques play an important role in a wide range of applications from memory devices to deep space explorations, and are expected to become even more important due to the rapid development in mobile phones and satellite-based communication.

In a general scenario, the sender encodes an N dimensional Boolean message vector $\boldsymbol{\xi}$, where $\xi_i \in (0,1),\ \forall i$, to an $M(>N)$ dimensional Boolean codeword $\boldsymbol{z}_0$, which is then being transmitted through a noisy communication channel. Noise corruption during transmission can be modelled by the noise vector $\boldsymbol{\zeta}$, where corrupted bits are marked by the value 1 and all other bits are zero, such that the received corrupted codeword takes the form $\boldsymbol{z} = \boldsymbol{z}_0 + \boldsymbol{\zeta}$ (mod 2). The received corrupted message is then decoded by the receiver for retrieving the original message $\boldsymbol{\xi}$.

The error-correcting ability comes at the expense of information redundancy. Shannon showed in his seminal work [1] that error-free communication is theoretically possible if the code rate, representing the fraction of informative bits in the transmitted codeword, is below the channel capacity; in the case of unbiased messages transmitted through a Binary Symmetric Channel (BSC), which we will focus on here, $R = N/M$ satisfies

$$R < 1 + p\log_2 p + (1-p)\log_2(1-p)\ . \tag{1}$$

The expression on the right is termed *Shannon's bound*. However, Shannon's derivation is non-constructive and the quest for codes which saturate Eq.(1) has been one of the central topics of information theory ever since.

In this paper we examine the efficiency and limitations of Gallager-type error-correcting code [2,3], which attracted much interest recently among researchers in this field. This code was discovered almost forty years ago by Gallager [2] but was abandoned shortly after its

invention due to the computational limitations of the time. Since their recent rediscovery by MacKay and Neal [3], different variations of Gallager-type codes have been developed [4–7] attempting to get as close as possible to saturating Shannon's bound.

In this paper we will examine the typical properties of a family of codes based on one variation, the MN code [3], using the established methods of statistical physics [8–11], to provide a theoretical study based on the typical performance of codes rather on the worst case analysis.

This paper is organised as follows: In the next two sections, we introduce Gallager-type error-correcting codes in detail and link them to the statistical mechanics framework. We then examine the equilibrium properties of various members of this family of codes using the replica method (section IV) and compare the bit-error rate below criticality. In section V, we examine the relation between Belief-Propagation (BP) decoding and the Thouless-Anderson-Palmer (TAP) approach to diluted spin systems; we then use it for comparing the analytical results obtained via the replica method to those obtained from simulations using BP decoding. In section VI we show a computationally efficient construction for one of the more practical constructions. Finally, we present conclusions for the current work and suggest future research directions.

II. GALLAGER-TYPE ERROR-CORRECTING CODES

There are several variations in Gallager-type error-correcting codes. The one discussed in this paper is termed the *MN* code, recently introduced by MacKay and Neal [3]. In these codes, a Boolean message $\boldsymbol{\xi}$ is encoded into a codeword $\boldsymbol{z}_0$ using two randomly constructed Boolean sparse matrices C_s and C_n, which are characterised in the following manner.

The rectangular sparse matrix C_s is of dimensionality $M \times N$, having randomly chosen K non-zero unit elements per row and C per column. The matrix C_n is an $M \times M$ (mod 2)-invertible matrix having randomly chosen L non-zero elements per row and column. These matrices are shared by the sender and the receiver.

Using these matrices, one can encode a message $\boldsymbol{\xi}$ into a codeword $\boldsymbol{z}_0$ in the following manner

$$\boldsymbol{z}_0 = C_n^{-1} C_s \boldsymbol{\xi} \pmod 2, \tag{2}$$

which is then transmitted via a noisy channel. Note that all matrix and vector components are Boolean $(0, 1)$, and all summations are carried out in this field. For simplicity, the noise process is modelled hereafter by a binary symmetric channel (BSC), where each bit is independently flipped with probability p. Extending the code presented here to other types of noise is straightforward.

During transmission, a noise vector $\boldsymbol{\zeta}$ is added to $\boldsymbol{z}_0$ and a corrupted codeword $\boldsymbol{z} = \boldsymbol{z}_0 + \boldsymbol{\zeta}$ (mod 2) is received at the other end of the channel. Decoding is then carried out by taking the product of the matrix C_n and the received codeword $\boldsymbol{z}$, which results in $C_s\boldsymbol{\xi} + C_n\boldsymbol{\zeta} = C_n\boldsymbol{z} \equiv \boldsymbol{J}$. The equation

$$C_s \boldsymbol{S} + C_n \boldsymbol{\tau} = \boldsymbol{J} \pmod 2, \tag{3}$$

is solved via the iterative methods of belief propagation (BP) [12,13] to obtain the most probable Boolean vectors $\boldsymbol{S}$ and $\boldsymbol{\tau}$. BP methods in this context have recently been shown to be identical to a TAP [14] based solution of a similar physical system [8].

III. A STATISTICAL MECHANICS PERSPECTIVE

Sourlas was the first to point out that error-correcting codes of this type have a similarity to Ising spin systems in statistical physics [15]; he demonstrated this using a simple version of the same nature. His work, that focused on extensively connected systems, was recently extended to finitely connected systems [9,11]. We follow a similar approach in the current investigation; preliminary results have already been presented in [10].

To facilitate the statistical physics analysis, we first employ the binary representation (± 1) of the dynamical variables $\boldsymbol{S}$ and $\boldsymbol{\tau}$ and of the check vector $\boldsymbol{J}$ rather than the Boolean one $(0, 1)$. The μ-th component of Eq.(3) is then rewritten as

$$\prod_{i\in\mathcal{L}_s(\mu)} S_i \prod_{j\in\mathcal{L}_n(\mu)} \tau_j = J_\mu, \tag{4}$$

where $\mathcal{L}_s(\mu)$ and $\mathcal{L}_n(\mu)$ are the sets of all indices of non-zero elements in row μ of the sparse matrices C_s and C_n, respectively. The check μ is given by message $\boldsymbol{\xi}$ and noise $\boldsymbol{\zeta}$ as $J_\mu = \prod_{i\in\mathcal{L}_s(\mu)} \xi_i \prod_{j\in\mathcal{L}_n(\mu)} \zeta_j$; it should be emphasised that the message vector $\boldsymbol{\xi}$ and the noise vector $\boldsymbol{\zeta}$ themselves are not known to the receiver.

An interesting link can now be formulated between the Bayesian framework of MN codes and Ising spin systems. Rewriting Kronecker's delta for binary variables x and y as $\delta[x;y] = (1+xy)/2 = \lim_{\beta\to\infty}\exp(-\beta\delta[-1;xy])$, one may argue that, using it as a likelihood, equation (4) gives rise to the conditional probability of the check $\boldsymbol{J}$ for given $\boldsymbol{S}$, $\boldsymbol{\tau}$, C_s and C_n

$$\mathcal{P}(\boldsymbol{J}|\boldsymbol{S},\boldsymbol{\tau},C_s,C_n) = \lim_{\beta\to\infty}\exp\left(-\beta\sum_{\mu=1}^{M}\delta[-1;J_\mu\prod_{i\in\mathcal{L}_s(\mu)}S_i\prod_{j\in\mathcal{L}_n(\mu)}\tau_j]\right). \tag{5}$$

Prior knowledge about possibly biased message and noise is represented by the prior distributions

$$\mathcal{P}_s(\boldsymbol{S}) = \frac{\exp\left(F_s\sum_{i=1}^{N}S_i\right)}{(2\cosh F_s)^N}, \quad \mathcal{P}_n(\boldsymbol{\tau}) = \frac{\exp\left(F_n\sum_{j=1}^{M}\tau_j\right)}{(2\cosh F_n)^M}, \tag{6}$$

respectively. Non-zero field F_s is introduced for biased message and F_n is determined by flip rate p of channel noise as $F_n = (1/2)\ln((1-p)/p)$. Using equations (5) and (6), the posterior distribution of $\boldsymbol{S}$ and $\boldsymbol{\tau}$ for given check $\boldsymbol{J}$ and matrices C_s and C_n is of the form

$$\begin{aligned}\mathcal{P}(\boldsymbol{S},\boldsymbol{\tau}|\boldsymbol{J},C_s,C_n) &= \frac{\mathcal{P}(\boldsymbol{J}|\boldsymbol{S},\boldsymbol{\tau},C_s,C_n)\mathcal{P}_s(\boldsymbol{S})\mathcal{P}_n(\boldsymbol{\tau})}{\mathcal{P}(\boldsymbol{J}|C_s,C_n)}\\ &= \lim_{\beta\to\infty}\frac{\exp\left(-\beta\mathcal{H}(\boldsymbol{S},\boldsymbol{\tau}|\boldsymbol{\mathcal{J}},\mathcal{D})\right)}{\mathcal{Z}(\boldsymbol{\mathcal{J}},\mathcal{D})},\end{aligned} \tag{7}$$

where $\mathcal{P}(\boldsymbol{J}|C_s,C_n) = \sum_{\{\boldsymbol{S},\boldsymbol{\tau}\}}\mathcal{P}(\boldsymbol{J}|\boldsymbol{S},\boldsymbol{\tau},C_s,C_n)\mathcal{P}_s(\boldsymbol{S})\mathcal{P}_n(\boldsymbol{\tau})$,

$$\begin{aligned}\mathcal{H}(\boldsymbol{S},\boldsymbol{\tau}|\boldsymbol{\mathcal{J}},\mathcal{D}) &= \sum_{\mu=1}^{M}\delta[-1;J_\mu\prod_{i\in\mathcal{L}_s(\mu)}S_i\prod_{j\in\mathcal{L}_n(\mu)}\tau_j] - \frac{F_s}{\beta}\sum_{i=1}^{N}S_i - \frac{F_n}{\beta}\sum_{j=1}^{M}\tau_j\\ &= \sum_{<i_1,..,i_K;j_1,..,j_L>}\mathcal{D}_{<i_1,..,i_K;j_1,..,j_L>}\delta\Big[-1;\mathcal{J}_{<i_1,..,i_K;j_1,..,j_L>}S_{i_1}\dots S_{i_K}\tau_{j_1}\dots\tau_{j_L}\Big]\\ &\quad -\frac{F_s}{\beta}\sum_{i=1}^{N}S_i - \frac{F_n}{\beta}\sum_{j=1}^{M}\tau_j\ ,\end{aligned} \tag{8}$$

and

$$\begin{aligned}\mathcal{Z}(\boldsymbol{\mathcal{J}},\mathcal{D}) &= \lim_{\beta\to\infty}\sum_{\{\boldsymbol{S},\boldsymbol{\tau}\}}\exp\left(-\beta\mathcal{H}(\boldsymbol{S},\boldsymbol{\tau}|\boldsymbol{\mathcal{J}},\mathcal{D})\right)\\ &= \sum_{\{\boldsymbol{S},\boldsymbol{\tau}\}}\prod_{<i_1,..,i_K;j_1,..,j_L>}\left[1+\frac{1}{2}\mathcal{D}_{\langle i_1,\cdots,i_K;j_1,\cdots,j_L\rangle}\left(\mathcal{J}_{<i_1,..,i_K;j_1,..,j_L>}S_{i_1}\ldots S_{i_K}\tau_{j_1}\ldots\tau_{j_L}-1\right)\right]\\ &\times\exp\left(F_s\sum_{i=1}^{N}S_i+F_n\sum_{j=1}^{M}\tau_j\right).\end{aligned} \tag{9}$$

The final form of posterior distribution (7) implies that the MN code is identical to an Ising spin system defined by the Hamiltonian (8) in the zero temperature limit $T=\beta^{-1}\to 0$. In equations (8) and (9), we introduced the sparse connectivity tensor $\mathcal{D}_{<i_1,..,j_L>}$ which takes the value 1 if the corresponding indices of both message and noise are chosen (i.e., if all corresponding indices of the matrices C_s and C_n are 1) and 0 otherwise, and coupling $\mathcal{J}_{<i_1,..,i_K;j_1,..,j_L>}=\xi_{i_1}\xi_{i_2}\ldots\xi_{i_K}\zeta_{j_1}\zeta_{j_2}\ldots\zeta_{j_L}$. These come to isolate the disorder in choosing the matrix connections, embedded in $\mathcal{D}_{<i_1,..,j_L>}$, and to simplify the notation.

The posterior distribution (7) can be used for decoding. One can show that expectation of the overlap between original message $\boldsymbol{\xi}$ and retrieved one $\hat{\boldsymbol{\xi}}$

$$m=\frac{1}{N}\sum_{i=1}^{N}\xi_i\hat{\xi}_i, \tag{10}$$

is maximised by setting $\hat{\boldsymbol{\xi}}$ to its Bayes-optimal estimator [16–19]

$$\hat{\xi}_i^B=\mathrm{sign}(m_i^S),\quad m_i^S=\sum_{\{\boldsymbol{S},\boldsymbol{\tau}\}}S_i\;\mathcal{P}(\boldsymbol{S},\boldsymbol{\tau}|\boldsymbol{J},C_s,C_n). \tag{11}$$

It is worth while noting that this optimal decoding is realized at *zero temperature* rather than at a *finite temperature* as in [17–19]. The reason is that the true likelihood term (5) corresponds to the *ground state* of the first term of the Hamiltonian (8) due to the existence of more degrees of freedom, in the form of the dynamical variables $\boldsymbol{\tau}$, which do not appear in other systems. Introducing the additional variables $\boldsymbol{\tau}$, the degrees of freedom in the spin system increase from N to $N+M$, while the number of constraints from the checks $\boldsymbol{J}$ remains M. This implies that in spite of the existence of quenched disorder caused by $\boldsymbol{\mathcal{J}}$ and $\mathcal{D}$, the system is free from frustration even in the low temperature limit, which is

useful for practical decoding using local search algorithms. The last two terms in Eq.(8) scale with β remain finite even in the zero temperature limit $\beta \to \infty$ representing the true prior distributions, which dominates the statistical properties of the system, while the first term vanishes to satisfy the parity check condition (4).

IV. EQUILIBRIUM PROPERTIES: THE REPLICA METHOD

As we use the methods of statistical mechanics, we concentrate on the case of long messages, in the of limit of $N, M \to \infty$ while keeping code rate $R = N/M = K/C$ finite. This limit is quite reasonable for this particular problem since Gallager-type codes are usually used in the transmission of long ($10^4 - 10^5$) messages, where finite size corrections are likely to be negligible.

Since the first part of the Hamiltonian (8) is invariant under the gauge transformation $S_i \to \xi_i S_i$, $\tau_j \to \zeta_j \tau_j$ and $\mathcal{J}_{\langle i_1,..,j_L\rangle} \to 1$, it is useful to decouple the correlation between the vectors $\boldsymbol{S}$, $\boldsymbol{\tau}$ and $\boldsymbol{\xi}$, $\boldsymbol{\zeta}$. Rewriting the Hamiltonian using this gauge, one obtains a similar expression to Eq.(8) apart from the second terms which become $F_s/\beta \sum_{i=1} \xi_i S_i$ and $F_n/\beta \sum_{j=1} \zeta_j \tau_j$.

Due to the existence of several types of quenched disorder in the system, it is natural to resort to replica method for investigating the typical properties in equilibrium. More specifically, we calculate expectation values of n-th power of partition function (9) with respect to the quenched variables $\boldsymbol{\xi}$, $\boldsymbol{\zeta}$ and $\mathcal{D}$ and take the limit $n \to 0$.

Carrying out the calculation in the zero temperature limit $\beta \to \infty$ gives rise to a set of order parameters

$$q_{\alpha,\beta,..,\gamma} = \left\langle \frac{1}{N} \sum_{i=1}^{N} Z_i \; S_i^{\alpha} \; S_i^{\beta}, .., S_i^{\gamma} \right\rangle_{\beta\to\infty}, \quad r_{\alpha,\beta,..,\gamma} = \left\langle \frac{1}{M} \sum_{i=1}^{M} Y_j \; \tau_j^{\alpha} \; \tau_j^{\beta}, .., \tau_j^{\gamma} \right\rangle_{\beta\to\infty} \tag{12}$$

where α, β, .. represent replica indices, and the variables Z_i and Y_j come from enforcing the restriction of C and L connections per index, respectively [9,20]:

$$\delta \left(\sum_{\langle i_2,..,i_K\rangle} \mathcal{D}_{<i,i_2,..,j_L>} - C \right) = \oint_0^{2\pi} \frac{dZ}{2\pi} \; Z^{\sum_{\langle i_2,..,i_K\rangle} \mathcal{D}_{<i,i_2,..,j_L>} - (C+1)} \; , \tag{13}$$

and similarly for the restriction on the j indices.

To proceed further, it is necessary to make an assumption about the order parameters symmetry. The assumption made here is that of replica symmetry in both the order parameters and the related conjugate variables

$$\begin{aligned} q_{\alpha,\beta..\gamma} &= a_q \int dx\ \pi(x)\ x^l\ ,\ \widehat{q}_{\alpha,\beta..\gamma} = a_{\widehat{q}} \int d\hat{x}\ \widehat{\pi}(\hat{x})\ \hat{x}^l \\ r_{\alpha,\beta..\gamma} &= a_r \int dy\ \rho(y)\ y^l\ ,\ \widehat{r}_{\alpha,\beta..\gamma} = a_{\widehat{r}} \int d\hat{y}\ \widehat{\rho}(\hat{y})\ \hat{y}^l\ , \end{aligned} \tag{14}$$

where l is the number of replica indices, a_* are normalisation coefficients, and $\pi(x), \widehat{\pi}(\hat{x}), \rho(y)$ and $\widehat{\rho}(\hat{y})$ represent probability distributions. Unspecified integrals are over the range $[-1, +1]$. This ansatz is supported by the facts that (i) the current system is free of frustration and (ii) there has never been observed replica symmetry breaking at Nishimori's condition [21] which corresponds to using correct priors F_s and F_n in our case [16]. The results obtained hereafter also support this ansatz. Extremizing the partition function with respect to distributions $\pi(\cdot)$, $\hat{\pi}(\cdot)$, $\rho(\cdot)$ and $\hat{\rho}(\cdot)$, one then obtains the free energy per spin

$$\begin{aligned} f &= -\frac{1}{N}\langle \ln \mathcal{Z} \rangle_{\xi,\zeta,\mathcal{D}} \\ &= \mathrm{extr}_{\{\pi,\hat{\pi},\rho,\rho\}} \Bigg\{ \frac{C}{K} \ln 2 + C \int dx\ d\hat{x}\ \pi(x)\ \hat{\pi}(\hat{x}) \ln(1 + x\hat{x}) + \frac{CL}{K} \int dy\ d\hat{y}\ \rho(y)\ \hat{\rho}(\hat{y}) \ln(1 + y\hat{y}) \\ &\quad - \frac{C}{K} \int \left[\prod_{k=1}^{K} dx_k \pi(x_k) \right] \left[\prod_{l=1}^{L} dy_l \rho(y_l) \right] \ln \left[1 + \prod_{k=1}^{K} x_k \prod_{l=1}^{L} y_l \right] \\ &\quad - \int \left[\prod_{k=1}^{C} d\hat{x}_k \hat{\pi}(\hat{x}_k) \right] \left\langle \ln \left[e^{F_s \xi} \prod_{k=1}^{C} (1 + \hat{x}_k) + e^{-F_s \xi} \prod_{k=1}^{C} (1 - \hat{x}_k) \right] \right\rangle_{\xi} \\ &\quad - \frac{C}{K} \int \left[\prod_{l=1}^{C} d\hat{y}_l \hat{\rho}(\hat{y}_l) \right] \left\langle \ln \left[e^{F_n \zeta} \prod_{l=1}^{L} (1 + \hat{y}_l) + e^{-F_n \zeta} \prod_{l=1}^{L} (1 - \hat{y}_l) \right] \right\rangle_{\zeta} \Bigg\}, \end{aligned} \tag{15}$$

where angled brackets with subscript $\boldsymbol{\xi}$, $\boldsymbol{\zeta}$ and $\mathcal{D}$ denote averages over the message and noise distributions respectively, and sparse connectivity tensor $\mathcal{D}$. Message averages take the form

$$\langle \cdots \rangle_{\xi} = \sum_{\xi = \pm 1} \frac{1 + \xi \tanh F_s}{2} (\cdots) \tag{16}$$

and similarly for $\langle \cdots \rangle_{\zeta}$. Details of the derivation are given in Appendix A.

Taking the functional variation of f with respect to the distributions π, $\hat{\pi}$, ρ and $\hat{\rho}$, one obtains the following saddle point equations

$$
\begin{aligned}
\pi(x) &= \int \prod_{l=1}^{C-1} d\hat{x}_l \; \hat{\pi}(\hat{x}_l) \left\langle \delta\left(x - \tanh\left(\xi F_s + \sum_{l=1}^{C-1} \tanh^{-1}\hat{x}_l\right)\right)\right\rangle_{\xi}, \\
\hat{\pi}(\hat{x}) &= \int \prod_{l=1}^{K-1} dx_l \; \pi(x_l) \int \prod_{l=1}^{L} dy_l \; \rho(y_l)\delta\left(\hat{x} - \prod_{l=1}^{K-1} x_l \prod_{l=1}^{L} y_l\right), \\
\rho(y) &= \int \prod_{l=1}^{L-1} d\hat{y}_l \; \hat{\rho}(\hat{y}_l) \left\langle \delta\left(y - \tanh\left(\zeta F_n + \sum_{l=1}^{L-1} \tanh^{-1}\hat{y}_l\right)\right)\right\rangle_{\zeta}, \\
\hat{\rho}(\hat{y}) &= \int \prod_{l=1}^{K} dx_l \; \pi(x_l) \int \prod_{l=1}^{L-1} dy_l \; \rho(y_l)\delta\left(\hat{y} - \prod_{l=1}^{K} x_l \prod_{l=1}^{L-1} y_l\right).
\end{aligned} \tag{17}
$$

After solving these equations, the expectation of the overlap between the message $\boldsymbol{\xi}$ and the Bayesian optimal estimator (11), which serves as a performance measure, can be evaluated as

$$
m = \frac{1}{N}\left\langle \sum_{i=1}^{N} \xi_i \mathrm{sign}\left\langle S_i \right\rangle_{\beta\to\infty} \right\rangle_{\boldsymbol{\xi},\boldsymbol{\zeta},\mathcal{D}} = \int dz \; \phi(z) \; \mathrm{sign}(z), \tag{18}
$$

where

$$
\phi(z) = \int \left[\prod_{l=1}^{C} d\hat{x}_l \; \hat{\pi}(\hat{x}_l)\right] \left\langle \delta\left(z - \tanh\left(F_s\xi + \sum_{i=1}^{C} \tanh^{-1}\hat{x}_i\right)\right)\right\rangle_{\xi}. \tag{19}
$$

The derivation of Eqs.(18) and (19) is given in Appendix B.

Examining the physical properties of the solutions for various connectivity values exposes significant differences between the various cases. In particular, these solutions fall into three different categories: the cases of $K = 1$ and general L value, the case of $K = L = 2$ and all other parameter values where either $K \geq 3$ or $L \geq 3$ (and $K > 1$). We describe the results obtained for each one of these cases separately.

A. Analytical solution - the case of $K \geq 3$ or $L \geq 3$, $K > 1$

Results for the cases of $K \geq 3$ or $L \geq 3$, $K > 1$ can be obtained analytically and have a simple and transparent interpretation; we will therefore focus first on this simple case. For unbiased messages (with $F_s = 0$), one can easily verify that the ferromagnetic phase, characterised by $m = 1$, and the probability distributions

$$
\pi(x) = \delta(x-1), \;\; \hat{\pi}(\hat{x}) = \delta(\hat{x}-1), \;\; \rho(y) = \delta(y-1), \;\; \hat{\rho}(\hat{y}) = \delta(\hat{y}-1) \; ; \tag{20}
$$

and the paramagnetic state of $m = 0$ with the probability distributions

$$\pi(x) = \delta(x),\ \hat{\pi}(\hat{x}) = \delta(\hat{x}),\ \hat{\rho}(\hat{y}) = \delta(\hat{y}),$$
$$\rho(y) = \frac{1+\tanh F_n}{2}\delta(y-\tanh F_n) + \frac{1-\tanh F_n}{2}\delta(y+\tanh F_n), \tag{21}$$

satisfy saddle point equations (17). Other solutions may be obtained numerically; here we have represented the distributions by $10^3 - 10^4$ bins and iterated Eqs.(17) $100 - 500$ times with 10^5 Monte Carlo sampling steps for each iteration. No solutions other than the above two have been discovered.

The thermodynamically-dominant state is found by evaluating the free energy of the two solutions using Eq.(15), which yields

$$f_{\rm ferro} = -\frac{C}{K} F_n \tanh F_n = -\frac{1}{R} F_n \tanh F_n, \tag{22}$$

for the ferromagnetic solution and

$$f_{\rm para} = \frac{C}{K}\ln 2 - \ln 2 - \frac{C}{K}\ln 2\cosh F_n = \frac{1}{R}\ln 2 - \ln 2 - \frac{1}{R}\ln 2\cosh F_n, \tag{23}$$

for the paramagnetic solution.

Figure 1(a) describes schematically the nature of the solutions for this case, in terms of the free energy and the magnetisation obtained, for various flip rate probabilities. The difference between the free energies of Eqs.(22) and (23)

$$f_{\rm ferro} - f_{\rm para} = \frac{\ln 2}{R}\left[R - 1 + H_2(p)\right], \tag{24}$$

vanishes in the boundary between the two phase

$$R_c = 1 - H_2(p) = 1 + p\log_2(p) + (1-p)\log_2(1-p), \tag{25}$$

which coincides with Shannon's channel capacity.

Equation (25) indicates that all constructions with either $K \geq 3$ or $L \geq 3$ (and $K > 1$) can potentially realize error-free data transmission for $R < R_c$ in the limit where both message and codeword lengths N and M become infinite, thus saturating Shannon's bound.

B. The case of $K = L = 2$

All codes with either $K = 3$ or $L = 3$, $K > 1$ potentially saturate Shannon's bound and are characterised by a first order phase transition between the ferromagnetic and paramagnetic solutions. On the other hand, numerical investigation based on Monte Carlo methods indicates of significantly different physical characteristics for $K = L = 2$ codes shown in Fig.1(b).

At the highest noise level, the paramagnetic solution (21) gives the unique extremum of the free energy until noise level reaches the first critical point p_1, at which the ferromagnetic solution (20) of higher free energy appears to be locally stable. As the noise level decreases, a second critical point p_2 appears, where the paramagnetic solution becomes unstable and a sub-optimal ferromagnetic solution and its mirror image emerge. Those solutions have lower free energy than the ferromagnetic solution until the noise level reaches the third critical point p_3. Below p_3, the ferromagnetic solution becomes the global minimum of the free energy, while the sub-optimal ferromagnetic solutions still remain locally stable. However, the sub-optimal solutions disappear at the spinodal point p_s and the ferromagnetic solution (and its mirror image) becomes the unique stable solution of the saddle point Eqs.(17) as shown by the numerical investigation for all $p < p_s$.

The analysis implies that p_3, the critical noise level below which the ferromagnetic solution becomes thermodynamically dominant, is lower than $p_c = H_2^{-1}(1-R)$ which corresponds to Shannon's bound. Namely, $K = L = 2$ does not saturate Shannon's bound in contrast to $K \geq 3$ codes even if optimally decoded. Nevertheless, it turns out that the free energy landscape, for noise levels $0 < p < p_s$, offers significant advantages in the decoding dynamic comparing to that of other codes ($K \geq 3$ or $L \geq 3$, $K > 1$).

C. General L codes with $K = 1$

The particular choice of $K = 1$, independently of the value chosen for L, exhibits a different behaviour presented schematically in Fig.1(c); also in this case there are no simple analytical solutions and all solutions in this scenario, except for the ferromagnetic solution, have been obtained numerically. The first important difference to be noted is that the paramagnetic state (21) is no longer a solution of the saddle point equations (17) and is being replaced by a sub-optimal ferromagnetic state. Convergence to the perfect solution of $m = 1$ can only be guaranteed for corruption rates smaller than that of the spinodal point, marking the maximal noise level for which only the ferromagnetic solution exists, $p < p_s$.

The $K = 1$ codes do not saturate Shannon's bound in general; however, we have found that at rates $R < 1/3$ they outperform the $K = L = 2$ code while offering slightly improved dynamical (decoding) properties. Studying the free energy in this case shows that as the corruption rate increases, sub-optimal ferromagnetic solutions (stable and unstable) emerge at the spinodal point p_s. When the noise increases further this sub-optimal state becomes the global minimum at p_1, dominating the system's thermodynamics. The transition at p_1 must occur at noise levels lower or equal to the value predicted by Shannon's bound. In Fig.2 we show free energy values computed for a given code rate and several values of L, marking Shannon's bound by a dashed line; it is clear that the thermodynamical transition observed numerically (i.e. the point where the ferromagnetic free energy equals the sub-optimal ferromagnetic free energy) is bellow, but very close, to the channel capacity. It implies that these codes also do not quite saturate Shannon's bound if optimally decoded but get quite close to it.

V. DECODING: BELIEF PROPAGATION/TAP APPROACH

The Bayesian message estimate (11) potentially provides the optimal retrieval of the original messages. However, it is computationally difficult to follow the prescription exactly

as it requires a sum over $\mathcal{O}(2^N)$ terms. Belief propagation [12,13] (BP) can be used for obtaining an approximate estimate. It was recently shown [8] that the BP algorithm can be derived, at least in the current context, from the TAP approach [14] to diluted systems in statistical mechanics.

Both algorithms (BP/TAP) are iterative methods which effectively calculate the marginal posterior probabilities $\mathcal{P}(S_i|\boldsymbol{J}, C_s, C_n) = \sum_{\{\{S_{k\neq i}\},\boldsymbol{\tau}\}} \mathcal{P}(\boldsymbol{S}, \boldsymbol{\tau}|\boldsymbol{J}, C_s, C_n)$ and $\mathcal{P}(\tau_j|\boldsymbol{J}, C_s, C_n) = \sum_{\{\boldsymbol{S},\{\tau_{k\neq j}\}\}} \mathcal{P}(\boldsymbol{S}, \boldsymbol{\tau}|\boldsymbol{J}, C_s, C_n)$ based on the following three assumptions:

1. The posterior distribution is factorizable with respect to dynamical variables $S_{i=1,\ldots,N}$ and $\tau_{j=1,\ldots,M}$.

2. The influence of check $J_{\mu=1,\ldots,M}$ on a specific site S_i (or τ_j) is also factorizable.

3. The contribution of a single variables $S_{i=1,\ldots,N}$, $\tau_{j=1,\ldots,M}$ and $J_{\mu=1,\ldots,M}$ to the macroscopic variables is small and can be isolated.

Parameterising pseudo-marginal posteriors and marginalized conditional probabilities as

$$\mathcal{P}(S_i|\{J_{\nu\neq\mu}\}, C_s, C_n) = \frac{1+m^S_{\mu i}S_i}{2}, \quad \mathcal{P}(\tau_j|\{J_{\nu\neq\mu}\}, C_s, C_n) = \frac{1+m^n_{\mu j}\tau_j}{2}, \tag{26}$$

$$\mathcal{P}(J_\mu|S_i, \{J_{\nu\neq\mu}\}, C_s, C_n) \sim \frac{1+\hat{m}^S_{\mu i}S_i}{2}, \quad \mathcal{P}(J_\mu|\tau_j, \{J_{\nu\neq\mu}\}, C_s, C_n) \sim \frac{1+\hat{m}^n_{\mu j}\tau_j}{2}, \tag{27}$$

the above assumptions provide a set of self-consistent equations [8,11]

$$m^S_{\mu l} = \tanh\left(F_s + \sum_{\nu\in\mathcal{M}_S(l)/\mu} \tanh^{-1}(\hat{m}^S_{\nu l})\right), \quad m^n_{\mu l} = \tanh\left(F_n + \sum_{\nu\in\mathcal{M}_n(l)/\mu} \tanh^{-1}(\hat{m}^n_{\nu l})\right). \tag{28}$$

and

$$\hat{m}^S_{\mu l} = J_\mu \prod_{k\in\mathcal{L}_S(\mu)/l} m^S_{\mu k} \prod_{j\in\mathcal{L}_n(\mu)} m^n_{\mu j}, \quad \hat{m}^n_{\mu l} = J_\mu \prod_{k\in\mathcal{L}_S(\mu)} m^S_{\mu k} \prod_{j\in\mathcal{L}_n(\mu)/l} m^n_{\mu j}. \tag{29}$$

Here, $\mathcal{M}_s(l)$ and $\mathcal{M}_n(l)$ indicate the set of all indices of non-zero components in the l-th column of the sparse matrices C_s and C_n, respectively. Similarly, $\mathcal{L}_s(\mu)$ and $\mathcal{L}_n(\mu)$ denote the set of all indices of non-zero components in μ-th row of the sparse matrices C_s and C_n, respectively. The notation $\mathcal{L}_s(\mu)/l$ represents the set of all indices belonging to $\mathcal{L}_s(\mu)$ except the index l.

Equations (28) and (29) are solved iteratively using the appropriate initial conditions. After obtaining a solution to all $m_{\mu l}$ and $\hat{m}_{\mu l}$, an approximated posterior mean can be calculated as

$$m_i^S = \tanh\left(F_s + \sum_{\mu\in\mathcal{M}_S(l)} \tanh^{-1}(\hat{m}_{\mu i}^S)\right), \tag{30}$$

which provides an approximation to the Bayes-optimal estimator (11) in the form of $\hat{\xi}^B = \text{sign}(m_i^S)$.

Notice that the rather vague meaning of the fields distributions introduced in the previous section becomes clear by introducing the new variables $x = \xi_i m_{\mu i}^S$, $\hat{x} = \xi_i \hat{m}_{\mu i}^S$, $y = \zeta_j m_{\mu j}^n$ and $\hat{y} = \zeta_j \hat{m}_{\mu j}^n$ [11]. If one considers that these variables are independently drawn from the distributions $\pi(x)$, $\hat{\pi}(\hat{x})$, $\rho(y)$ and $\hat{\rho}(\hat{y})$, the replica symmetric saddle point equations (17) are recovered from the BP/TAP equations (28) and (29). This connection can be extended to the free energy as equations (28) and (29) extremize the TAP free energy

$$\begin{aligned} f_{\text{TAP}}(\{\boldsymbol{m}\},\{\hat{\boldsymbol{m}}\}) = {} & \frac{M}{N}\ln 2 + \frac{1}{N}\sum_{\mu=1}^{M}\sum_{i\in\mathcal{L}_S(\mu)} \ln\left(1 + m_{\mu i}^S \hat{m}_{\mu i}^S\right) + \frac{1}{N}\sum_{\mu=1}^{M}\sum_{j\in\mathcal{L}_n(\mu)} \ln\left(1 + m_{\mu j}^n \hat{m}_{\mu j}^n\right) \\ & -\frac{1}{N}\sum_{\mu=1}^{M} \ln\left(1 + J_\mu \prod_{i\in\mathcal{L}_S(\mu)} m_{\mu i}^S \prod_{j\in\mathcal{L}_n(\mu)} m_{\mu j}^n\right) \\ & -\frac{1}{N}\sum_{i=1}^{N} \ln\left[e^{F_s}\prod_{\mu\in\mathcal{M}_S(i)}\left(1+\hat{m}_{\mu i}^S\right) + e^{-F_s}\prod_{\mu\in\mathcal{M}_S(i)}\left(1-\hat{m}_{\mu i}^S\right)\right] \\ & -\frac{1}{N}\sum_{j=1}^{M} \ln\left[e^{F_n}\prod_{\mu\in\mathcal{M}_n(j)}\left(1+\hat{m}_{\mu j}^n\right) + e^{-F_n}\prod_{\mu\in\mathcal{M}_n(j)}\left(1-\hat{m}_{\mu j}^n\right)\right] . \end{aligned} \tag{31}$$

This expression may be used for selecting the thermodynamically dominant state when Eqs.(28) and (29) have several solutions.

We have investigated the performance of the various codes using BP/TAP equations as the decoding algorithm. Solutions have been obtained by iterating the equations (28) and (29) $100-500$ times under various initial conditions. Since the system is not frustrated, the dynamics converges within $10-30$ updates in most cases except close to criticality. The numerical results mirror the behaviour predicted by the analytical solutions.

For either $K \geq 3$ or $L \geq 3$,$K > 1$ codes, the ferromagnetic solution

$$m^S_{\mu i} = \xi_i, \quad \hat{m}^S_{\mu i} = \xi_i, \quad m^n_{\mu j} = \zeta_j, \quad \hat{m}^n_{\mu j} = \zeta_j, \tag{32}$$

which provides perfect decoding ($m = 1$) and the paramagnetic solution ($m = 0$)

$$m^S_{\mu i} = 0, \quad \hat{m}^S_{\mu i} = 0, \quad m^n_{\mu j} = \tanh F_n = 1 - 2p, \quad \hat{m}^n_{\mu j} = 0 \ , \tag{33}$$

are obtained in various runs depending on the initial conditions (the message is assumed unbiased resulting in $F_s = 0$). However, it is difficult to set the initial conditions within the basin of attraction of the ferromagnetic solution without prior knowledge about the transmitted message $\boldsymbol{\xi}$.

Biased coding is sometimes used for alleviating this difficulty [3]. Using a redundant source of information (equivalent to the introduction of a non-zero field F_s in the statistical physics description), one effectively increases the probability of the initial conditions being closer to the ferromagnetic solution. The main drawback of this method is that the information per transmitted bit is significantly reduced due to this redundancy. In order to investigate how the maximum performance is affected by transmitting biased messages, we have evaluated the critical information rate (i.e., code rate $\times H_2(f_s = (1 + \tanh F_s)/2)$, the source redundancy), below which the ferromagnetic solution becomes thermodynamically dominant [Fig.3(a)]. The data were obtained by the BP/TAP method (diamonds) and numerical solutions of from replica framework (square); the dominant solution in the BP/TAP results, was selected by using the free energy (31). Numerical solutions have been obtained using $10^3 - 10^4$ bin models for each distribution and had been run for 10^5 steps per noise level. The various results are highly consistent and practically saturate Shannon's bound for the same noise level. However, it is important to point out that close to Shannon's limit, prior knowledge on the original message is required for setting up appropriate initial conditions that ensure convergence to the ferromagnetic solution; such prior knowledge is not available in practice.

Although $K, L \geq 3$ codes seem to offer optimal performance when highly biased messages are transmitted, this seems to be of little relevance in most cases, characterised by the transmission of compressed unbiased messages or only slightly biased messages. In this

sense, $K = L = 2$ and $K = 1$ codes can be considered more practical as the BP/TAP dynamics of these codes exhibit unique convergence to the ferromagnetic solution (or mirror image in the $K = L = 2$ case) from *any* initial condition up to a certain noise level. This property results from the fact that the corresponding free energies have no local minima other than the ferromagnetic solution below p_s.

In figures 3(b) and (c) we show the value of p_s for the cases of $K = L = 2$ and $K = 1$, $L = 2$ respectively, evaluated by numerical solutions from the replica framework (diamonds) and using the BP/TAP method.

The case of $K = L = 2$ shows consistent successful decoding for the code rates examined and up to noise levels slightly below, but close to, Shannon's bound. It should be emphasised here that initial conditions are chosen almost randomly in the BP/TAP method, with a very slight bias of $\mathcal{O}(10^{-12})$ in the initial magnetisation. This result suggests using $K = L = 2$ codes (or similar), rather than $K, L \geq 3$ codes, although the latter may potentially have better equilibrium properties.

In Fig.3(c) we show that for code rates $R < 1/3$, codes parametrised by $K = 1$ and $L = 2$ outperform $K = L = 2$ codes with one additional advantage: Due to the absence of mirror symmetries these codes converge to the ferromagnetic state much faster, and there is no risk of convergence to the mirror solution. The difference in performance becomes even larger as the code rate decreases. Higher code rates will result in performance deterioration due to the low connectivity, eventually bringing the system below the percolation threshold.

In Fig.4 we examine the dependence of the noise level of the spinodal point p_s on the value of L, and show that the choice of $L = 2$ is optimal within this family. Codes with $L = 1$ have very poor error-correction capabilities as their Hamiltonian (8) corresponds to the Mattis model, which is equivalent to a simple ferromagnet in a random field attaining magnetisation $m = 1$ only in the noiseless case.

VI. REDUCING ENCODING COSTS

The BP/TAP algorithm already offers an efficient decoding method, which requires $\mathcal{O}(N)$ operations; however, the current encoding scheme includes three costly processes: (a) The computational cost of constructing the generating matrix $C_n^{-1}C_s$ requires $\mathcal{O}(N^3)$ operations for inverting the matrix C_n and $\mathcal{O}(N^2)$ operations for the matrix multiplication. (b) The memory allocation for generating the matrix $C_n^{-1}C_s$ scales as $\mathcal{O}(N^2)$ since this matrix is typically dense. (c) The encoding itself $\boldsymbol{z}_0 = C_n^{-1}C_s\boldsymbol{\xi}$ (mod 2) requires $\mathcal{O}(N^2)$ operations.

These computational costs become significant when long messages $N = 10^4 \sim 10^5$ are transmitted, which is typically the case for which Gallager-type codes are being used. This may require long encoding times and may delay the transmission.

These problems may be solved by utilising systematically constructed matrices instead of random ones, of some similarity to the constructions of [4]. Here, we present a simple method to reduce the computational and memory costs to $\mathcal{O}(N)$ for $K = L = 2$ and $K = 1$, $L = 2$ codes. Our proposal is mainly based on using a specific matrix for C_n,

$$\bar{C}_n = \begin{pmatrix} 1 & 0 & 0 & 0 & \cdots & 0 & 0 \\ 1 & 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 1 & 1 \end{pmatrix}, \tag{34}$$

instead of a randomly-constructed one. For C_s, we use a random matrix of $K = 2$ (or $K = 1$) non-zero elements per row as before.

The inverse (mod 2) of $\bar{C}_n^{-1}$ becomes the lower triangular matrix

$$\bar{C}_n^{-1} = \begin{pmatrix} 1 & 0 & 0 & 0 & \cdots & 0 & 0 \\ 1 & 1 & 0 & 0 & \cdots & 0 & 0 \\ 1 & 1 & 1 & 0 & \cdots & 0 & 0 \\ 1 & 1 & 1 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \ddots & \vdots & \vdots \\ 1 & 1 & 1 & 1 & \cdots & 1 & 1 \end{pmatrix} . \tag{35}$$

This suggests that encoding the message $\boldsymbol{\xi}$ into a codeword $\boldsymbol{z}^0$ would require only $\mathcal{O}(N)$ operations by carrying it out in two steps

$$t_\mu = (C_s \boldsymbol{\xi})_\mu \pmod 2, \quad \text{for } \mu = 1, 2, \ldots, M, \tag{36}$$

$$z_\mu^0 = (\bar{C}_n^{-1} \boldsymbol{t})_\mu = z_{\mu-1}^0 + t_\mu \pmod 2, \quad \text{for } \mu = 2, \ldots, M, \tag{37}$$

with $z_1^0 = t_1$. Both steps require $\mathcal{O}(N)$ operations due to the sparse nature of C_s. In addition, the required memory resources are also reduced to $\mathcal{O}(N)$ since only the sparse matrix C_s should be stored.

The possible drawback of using the systematic matrix (34) is a deterioration in the error correction ability. We have examined numerically the performance of new construction to discover, to our surprise, that it is very similar to that of random matrix based codes as shown in Table I. Although our examination is only limited to BSC and i.i.d. messages, it seems to suggest that some deterministically constructed matrices may be implemented successfully in practice.

VII. SUMMARY

In this paper, we have investigated the typical performance of the MN codes, a variation of Gallager-type error-correcting codes, by mapping them onto Ising spin models and making use of the established methods of statistical physics. We have discovered that for a certain choice of parameters, either $K \geq 3$ or $L \geq 3$, $K > 1$ these codes potentially saturate the channel capacity, although this cannot be used efficiently in practice due to the decrease in

the basin of attraction which typically diverts the decoding dynamics towards the undesired paramagnetic solution.

Codes with $K = 2$ and $L = 2$ show close to optimal performance while keeping a large basin of attraction, resulting in more practical codes. Constructions of the form $K = 1$, $L = 2$ outperform the $K = L = 2$ codes for code rates $R < 1/3$, having improved dynamical properties.

These results are complementary to those obtained so far by the information theory community and seem to indicate that worst-case analysis can be, in some situations, too pessimistic when compared to the typical performance results.

Beyond the theoretical aspects, we proposed an efficient method for reducing the computational costs and the required memory allocation by using a specific construction of the matrix C_n. These codes are highly attractive and provide lower computational costs for both encoding and decoding.

Various aspects that remain to be studied include a proper analysis of the finite size effects for rates below and above the channel capacity, which are of great practical relevance; and the use of statistical physics methods for optimising the matrix constructions.

ACKNOWLEDGEMENT

Support by the JSPS RFTF program (YK), The Royal Society and EPSRC grant GR/N00562 (DS) is acknowledged.

APPENDIX A: REPLICA FREE ENERGY

The purpose of this appendix is to derive the averaged free energy per spin (15). Applying the gauge transformation

$$\begin{aligned} J_\mu &\to J_\mu \prod_{i\in\mathcal{L}_s(\mu)} \xi_i \prod_{j\in\mathcal{L}_n(\mu)} \zeta_j = 1 \\ S_i &\to S_i\xi_i \\ \tau_j &\to \tau_j\zeta_j, \end{aligned} \tag{A1}$$

to eq. (9), one may rewrite the partition function in the form

$$\begin{aligned} \mathcal{Z}(\boldsymbol{\xi},\boldsymbol{\zeta},\mathcal{D}) &= \sum_{\boldsymbol{S},\boldsymbol{\tau}} \exp\left(F_s\sum_{i=1}^{N}\xi_i S_i + F_n\sum_{j=1}^{M}\zeta_j\tau_j\right) \\ \times \prod_{\langle i_1,\cdots,i_K;j_1,\cdots,j_L\rangle} &\left[1-\mathcal{D}_{\langle i_1,\cdots,i_K;j_1,\cdots,j_L\rangle} + \mathcal{D}_{\langle i_1,\cdots,i_K;j_1,\cdots,j_L\rangle}\frac{1}{2}\left(1+S_{i_1}\cdots S_{i_K}\tau_{j_1}\cdots\tau_{j_L}\right)\right]. \end{aligned} \tag{A2}$$

Using the replica method, one calculates the quenched average of the n-th power of the partition function given by

$$\begin{aligned} \langle\mathcal{Z}(\boldsymbol{\xi},\boldsymbol{\zeta},\mathcal{D})^n\rangle_{\boldsymbol{\xi},\boldsymbol{\zeta},\mathcal{D}} &= \sum_{\boldsymbol{S}^1\cdots\boldsymbol{S}^n}\sum_{\boldsymbol{\tau}^1\cdots\boldsymbol{\tau}^n} \left\langle\exp\left(F_s\sum_{i=1}^{N}\xi_i\sum_{\alpha=1}^{n}S_i^\alpha\right)\right\rangle_{\boldsymbol{\xi}} \left\langle\exp\left(F_n\sum_{j=1}^{M}\zeta_j\sum_{\alpha=1}^{n}\tau_i^\alpha\right)\right\rangle_{\boldsymbol{\zeta}} \\ \times \left\langle\prod_{\langle i_1,\cdots,i_K;j_1,\cdots,j_L\rangle}\prod_{\alpha=1}^{n}\left\{1+\frac{1}{2}\mathcal{D}_{\langle i_1,\cdots,i_K;j_1,\cdots,j_L\rangle}\left(S_{i_1}^\alpha\cdots S_{i_K}^\alpha\tau_{j_1}^\alpha\cdots\tau_{j_L}^\alpha-1\right)\right\}\right\rangle_{\mathcal{D}}, \end{aligned} \tag{A3}$$

where averages with respect to $\boldsymbol{\xi}$ can be easily performed

$$\begin{aligned} \left\langle\exp\left(F_s\sum_{i=1}^{N}\xi_i\sum_{\alpha=1}^{n}S_i^\alpha\right)\right\rangle_{\boldsymbol{\xi}} &= \prod_{i=1}^{N}\left[\left(\frac{1+\tanh F_s}{2}\right)e^{F_s\sum_{\alpha=1}^{n}S_i^\alpha} + \left(\frac{1-\tanh F_s}{2}\right)e^{-F_s\sum_{\alpha=1}^{n}S_i^\alpha}\right] \\ &= \prod_{i=1}^{N}\left\langle\exp\left(\xi F_s\sum_{a=1}^{n}S_i^a\right)\right\rangle_{\xi}, \end{aligned} \tag{A4}$$

and similarly for $\langle\cdots\rangle_{\boldsymbol{\zeta}}$. The main problem is in averages over the sparse tensor realisations $\mathcal{D}$, which have complicated constraints. Following the procedure introduced by Wong and Sherrington [20], it is being rewritten as

$$\left\langle\prod_{\langle i_1,\cdots,i_K;j_1,\cdots,j_L\rangle}\prod_{\alpha=1}^{n}\left[1+\frac{1}{2}\mathcal{D}_{\langle i_1,\cdots,i_K;j_1,\cdots,j_L\rangle}\left(S_{i_1}^\alpha\cdots S_{i_K}^\alpha\tau_{j_1}^\alpha\cdots\tau_{j_L}^\alpha-1\right)\right]\right\rangle_{\mathcal{D}}$$

$$= \mathcal{N}^{-1} \sum_{\mathcal{D}} \prod_{i=1}^{N} \delta \left(\sum_{\langle i_1,\cdots,i_K;j_1,\cdots,j_L\rangle} \mathcal{D}_{\langle i,i_2,\cdots,i_K;j_1,\cdots,j_L\rangle} - C \right) \prod_{j=1}^{M} \delta \left(\sum_{\langle i_1,\cdots,i_K;j_1,\cdots,j_L\rangle} \mathcal{D}_{\langle i_1,\cdots,i_K;j,j_2,\cdots,j_L\rangle} - L \right)$$
$$\times \prod_{\langle i_1,\cdots,i_K;j_1,\cdots,j_L\rangle} \prod_{\alpha=1}^{n} \left[1 + \frac{1}{2} \mathcal{D}_{\langle i_1,\cdots,i_K;j_1,\cdots,j_L\rangle} \left(S_{i_1}^{\alpha} \cdots S_{i_K}^{\alpha} \tau_{j_1}^{\alpha} \cdots \tau_{j_L}^{\alpha} - 1 \right) \right], \quad \text{(A5)}$$

where $\delta(\cdots)$ represents Dirac's δ-function and

$$\mathcal{N} = \sum_{\mathcal{D}} \prod_{i=1}^{N} \delta \left(\sum_{\langle i_2,\cdots,i_K;j_1,\cdots,j_L\rangle} \mathcal{D}_{\langle i,i_2,\cdots,i_K;j_1,\cdots,j_L\rangle} - C \right) \prod_{j=1}^{M} \delta \left(\sum_{\langle i_1,\cdots,i_K;j_2,\cdots,j_L\rangle} \mathcal{D}_{\langle i_1,\cdots,i_K;j,j_2,\cdots,j_L\rangle} - L \right) \quad \text{(A6)}$$

represents the normalisation constant.

We first evaluate this normalisation constant using the integral representation of the δ-function and Eq.(A6), to obtain

$$\begin{aligned}
\mathcal{N} &= \sum_{\mathcal{D}} \prod_{i=1}^{N} \delta \left(\sum_{\langle i_2,\cdots,i_K;j_1,\cdots,j_L\rangle} \mathcal{D}_{\langle i,i_2,\cdots,i_K;j_1,\cdots,j_L\rangle} - C \right) \prod_{j=1}^{M} \delta \left(\sum_{\langle i_1,\cdots,i_K;j_2,\cdots,j_L\rangle} \mathcal{D}_{\langle i_1,\cdots,i_K;j,j_2,\cdots,j_L\rangle} - L \right) \\
&= \sum_{\mathcal{D}} \prod_{i=1}^{N} \left\{ \int_0^{2\pi} \frac{d\lambda_i}{2\pi} \exp \left[i\lambda_i \left(\sum_{\langle i_2,\cdots,i_K;j_1,\cdots,j_L\rangle} \mathcal{D}_{\langle i,i_2,\cdots,i_K;j_1,\cdots,j_L\rangle} - C \right) \right] \right\} \\
&\quad \times \prod_{j=1}^{M} \left\{ \int_0^{2\pi} \frac{d\lambda_j}{2\pi} \exp \left[i\lambda_j \left(\sum_{\langle i_1,\cdots,i_K;j_2,\cdots,j_L\rangle} \mathcal{D}_{\langle i_1,\cdots,i_K;j,j_2,\cdots,j_L\rangle} - L \right) \right] \right\} \\
&= \prod_{i=1}^{N} \left\{ \int_0^{2\pi} \frac{d\lambda_i}{2\pi} e^{-iC\lambda_i} \right\} \prod_{j=1}^{M} \left\{ \int_0^{2\pi} \frac{d\nu_j}{2\pi} e^{-iL\nu_j} \right\} \\
&\quad \times \sum_{\mathcal{D}} \prod_{i=1}^{N} \left\{ \prod_{\langle i_2,\cdots,i_K;j_1,\cdots,j_L\rangle} e^{i\lambda_i \mathcal{D}_{\langle i,i_2,\cdots,i_K;j_1,\cdots,j_L\rangle}} \right\} \prod_{j=1}^{M} \left\{ \prod_{\langle i_1,\cdots,i_K;j_2,\cdots,j_L\rangle} e^{i\nu_j \mathcal{D}_{\langle i_1,\cdots,i_K;j,j_2,\cdots,j_L\rangle}} \right\} \\
&= \prod_{i=1}^{N} \left\{ \int_0^{2\pi} \frac{d\lambda_i}{2\pi} e^{-iC\lambda_i} \right\} \prod_{j=1}^{M} \left\{ \int_0^{2\pi} \frac{d\nu_j}{2\pi} e^{-iL\nu_j} \right\} \\
&\quad \times \sum_{\mathcal{D}} \prod_{\langle i_1,\cdots,i_K;j_1,\cdots,j_L\rangle} \left\{ \left(e^{i\lambda_{i_1}} \cdots e^{i\lambda_{i_K}} e^{i\nu_{j_1}} \cdots e^{i\nu_{j_L}} \right)^{\mathcal{D}_{\langle i_1,\cdots,i_K;j_1,\cdots,j_L\rangle}} \right\} \\
&= \prod_{i=1}^{N} \left\{ \oint \frac{dZ_i}{2\pi i} Z_i^{-(C+1)} \right\} \prod_{j=1}^{M} \left\{ \oint \frac{dY_j}{2\pi i} Y_j^{-(L+1)} \right\} \prod_{\langle i_1,\cdots,i_K;j_1,\cdots,j_L\rangle} \left(1 + Z_{i_1} \cdots Z_{i_K} Y_{j_1} \cdots Y_{j_L} \right), \quad \text{(A7)}
\end{aligned}$$

where we made use of the transformations $Z_i = e^{i\lambda_i}, Y_j = e^{i\nu_j}$, and carried out summations with respect to the realisation of $\mathcal{D}$. Expanding the product on the right hand side one obtains

$$\prod_{\langle i_1,\cdots,i_K;j_1,\cdots,j_L\rangle} \left[1 + \left(Z_{i_1} \cdots Z_{i_K} Y_{j_1} \cdots Y_{j_L} \right) \right]$$

$$= \exp\left[\sum_{\langle i_1,\cdots,i_K;j_1,\cdots,j_L\rangle} \ln\left\{1+(Z_{i_1}\cdots Z_{i_K}Y_{j_1}\cdots Y_{j_L})\right\}\right]$$
$$\simeq \exp\left[\sum_{\langle i_1,\cdots,i_K;j_1,\cdots,j_L\rangle} (Z_{i_1}\cdots Z_{i_K}Y_{j_1}\cdots Y_{j_L})\right]$$
$$\simeq \exp\left[\frac{1}{K!}\left(\sum_{i=1}^{N} Z_i\right)^K \frac{1}{L!}\left(\sum_{j=1}^{M} Y_j\right)^L\right], \tag{A8}$$

in the thermodynamic limit. Using the identities

$$1 = \int dq\ \delta\left(\sum_{i=1}^{N} Z_i - q\right), \quad 1 = \int dr\ \delta\left(\sum_{j=1}^{M} Y_j - r\right) \tag{A9}$$

Eq. (A7) becomes

$$\begin{aligned}
\mathcal{N} &= \int dq\ \delta\left(\sum_{i=1}^{N} Z_i - q\right)\int dr\ \delta\left(\sum_{j=1}^{M} Y_j - r\right) \\
&\quad\times \prod_{i=1}^{N}\left\{\oint \frac{dZ_i}{2\pi i} Z_i^{-(C+1)}\right\}\prod_{j=1}^{M}\left\{\oint \frac{dY_j}{2\pi i} Y_j^{-(L+1)}\right\}\exp\left(\frac{q^K}{K!}\frac{r^L}{L!}\right) \\
&= \int dq \int \frac{d\hat{q}}{2\pi i}\exp\left[\hat{q}\left(\sum_{i=1}^{N} Z_i - q\right)\right]\int dr\int \frac{d\hat{r}}{2\pi i}\exp\left[\hat{r}\left(\sum_{j=1}^{M} Y_j - r\right)\right] \\
&\quad\times \prod_{i=1}^{N}\left\{\oint \frac{dZ_i}{2\pi i} Z_i^{-(C+1)}\right\}\prod_{j=1}^{M}\left\{\oint \frac{dY_j}{2\pi i} Y_j^{-(L+1)}\right\}\exp\left(\frac{q^K}{K!}\frac{r^L}{L!}\right) \\
&= \int dq \int \frac{d\hat{q}}{2\pi i}\int dr\int \frac{d\hat{r}}{2\pi i}\exp\left(\frac{q^K}{K!}\frac{r^L}{L!} - q\hat{q} - r\hat{r}\right) \\
&\quad\times \prod_{i=1}^{N}\left[\oint \frac{dZ_i}{2\pi i} Z_i^{-(C+1)}\exp\left(\hat{q}Z_i\right)\right]\prod_{j=1}^{M}\left[\oint \frac{dY_j}{2\pi i} Y_j^{-(L+1)}\exp\left(\hat{r}Y_j\right)\right] .
\end{aligned} \tag{A10}$$

The contour integrals provide the following constants

$$\prod_{i=1}^{N}\left[\oint \frac{dZ_i}{2\pi i} Z_i^{-(C+1)}\exp\left(\hat{q}Z_i\right)\right] = \left(\frac{\hat{q}^C}{C!}\right)^N, \quad \prod_{j=1}^{M}\left[\oint \frac{dY_j}{2\pi i} Y_j^{-(L+1)}\exp\left(\hat{r}Y_j\right)\right] = \left(\frac{\hat{r}^L}{L!}\right)^M, \tag{A11}$$

respectively. Applying the saddle point method to the remaining integrals, one obtains

$$\mathcal{N} = \mathrm{extr}_{\{q,\hat{q},r,\hat{r}\}}\left\{\exp\left[\frac{q^K}{K!}\frac{r^L}{L!} - q\hat{q} - r\hat{r} + NC\ln\hat{q} - N\ln(C!) + ML\ln\hat{r} - M\ln(L!)\right]\right\}, \tag{A12}$$

which yields the following saddle point equations with respect to q, r, $\hat{q}$ and $\hat{r}$

$$\begin{aligned}
q &= \frac{NC}{\hat{q}}, \quad r = \frac{ML}{\hat{r}} \\
\hat{q} &= \frac{q^{K-1}}{(K-1)!}\frac{r^L}{L!}, \quad \hat{r} = \frac{r^{L-1}}{(L-1)!}\frac{q^K}{K!} ,
\end{aligned} \tag{A13}$$

providing the normalisation constant

$$\mathcal{N} = \left(\frac{\hat{q}^C}{C!}\right)^N \left(\frac{\hat{r}^L}{L!}\right)^M \exp\left(\frac{q^K}{K!}\frac{r^L}{L!} - q\hat{q} - r\hat{r}\right) \ . \tag{A14}$$

Equation (A5) can be evaluated similarly. Following a similar calculation to that of Eq.(A7) provides

$$\begin{aligned}
&\left\langle \prod_{\langle i_1,\cdots,i_K;j_1,\cdots,j_L\rangle} \prod_{\alpha=1}^{n} \left\{1 + \frac{1}{2}\mathcal{D}_{\langle i_1,\cdots,i_K;j_1,\cdots,j_L\rangle}\left(S_{i_1}^{\alpha}\cdots S_{i_K}^{\alpha}\tau_{j_1}^{\alpha}\cdots\tau_{j_L}^{\alpha} - 1\right)\right\}\right\rangle_{\mathcal{D}} \\
&= \mathcal{N}^{-1}\prod_{i=1}^{N}\left\{\oint \frac{dZ_i}{2\pi i} Z_i^{-(C+1)}\right\}\prod_{j=1}^{M}\left\{\oint \frac{dY_j}{2\pi i} Y_j^{-(L+1)}\right\} \\
&\quad\times \prod_{\langle i_1,\cdots,i_K;j_1,\cdots,j_L\rangle}\left[1 + (Z_{i_1}\cdots Z_{i_K}Y_{j_1}\cdots Y_{j_L})\prod_{\alpha=1}^{n}\frac{1}{2}\left(1 + S_{i_1}^{\alpha}\cdots S_{i_K}^{\alpha}\tau_{j_1}^{\alpha}\cdots\tau_{j_L}^{\alpha}\right)\right].
\end{aligned} \tag{A15}$$

Using the expansion

$$\begin{aligned}
&\prod_{\alpha=1}^{n}\left(1 + S_{i_1}^{\alpha}\cdots S_{i_K}^{\alpha}\tau_{j_1}^{\alpha}\cdots\tau_{j_L}^{\alpha}\right) \\
&= 1 + \sum_{\alpha=1}^{n} S_{i_1}^{\alpha}\cdots S_{i_K}^{\alpha}\tau_{j_1}^{\alpha}\cdots\tau_{j_L}^{\alpha} + \sum_{\langle\alpha_1,\alpha_2\rangle}(S_{i_1}^{\alpha_1}S_{i_1}^{\alpha_2})\cdots(S_{i_K}^{\alpha_1}S_{i_K}^{\alpha_2})(\tau_{j_1}^{\alpha_1}\tau_{j_1}^{\alpha_2})\cdots(\tau_{j_L}^{\alpha_1}\tau_{j_L}^{\alpha_2}) \\
&\quad + \cdots + \sum_{\langle\alpha_1,\cdots,\alpha_n\rangle}(S_{i_1}^{\alpha_1}\cdots S_{i_1}^{\alpha_n})\cdots(S_{i_K}^{\alpha_1}\cdots S_{i_K}^{\alpha_n})(\tau_{j_1}^{\alpha_1}\cdots\tau_{j_1}^{\alpha_n})\cdots(\tau_{j_L}^{\alpha_1}\cdots\tau_{j_L}^{\alpha_n}) \\
&= \sum_{m=0}^{n}\sum_{\langle\alpha_1,\cdots,\alpha_m\rangle}(S_{i_1}^{\alpha_1}\cdots S_{i_1}^{\alpha_m})\cdots(S_{i_K}^{\alpha_1}\cdots S_{i_K}^{\alpha_m})(\tau_{j_1}^{\alpha_1}\cdots\tau_{j_1}^{\alpha_m})\cdots(\tau_{j_L}^{\alpha_1}\cdots\tau_{j_L}^{\alpha_m}),
\end{aligned} \tag{A16}$$

resulting in

$$\begin{aligned}
&\prod_{\langle i_1,\cdots,i_K;j_1,\cdots,j_L\rangle}\left[1 + (Z_{i_1}\cdots Z_{i_K}Y_{j_1}\cdots Y_{j_L})\prod_{\alpha=1}^{n}\frac{1}{2}\left(1 + S_{i_1}^{\alpha}\cdots S_{i_K}^{\alpha}\tau_{j_1}^{\alpha}\cdots\tau_{j_L}^{\alpha}\right)\right] \\
&\simeq e^{\sum_{\langle i_1,\cdots,i_K;j_1,\cdots,j_L\rangle} Z_{i_1}\cdots Z_{i_K}Y_{j_1}\cdots Y_{j_L}\prod_{\alpha=1}^{n}\frac{1}{2}\left(1+S_{i_1}^{\alpha}\cdots S_{i_K}^{\alpha}\tau_{j_1}^{\alpha}\cdots\tau_{j_L}^{\alpha}\right)} \\
&= e^{\frac{1}{2^n}\sum_{\langle i_1,\cdots,i_K;j_1,\cdots,j_L\rangle} Z_{i_1}\cdots Z_{i_K}Y_{j_1}\cdots Y_{j_L}\sum_{m=0}^{n}\sum_{\langle\alpha_1,\cdots,\alpha_m\rangle}(S_{i_1}^{\alpha_1}\cdots S_{i_1}^{\alpha_m})\cdots(S_{i_K}^{\alpha_1}\cdots S_{i_K}^{\alpha_m})(\tau_{j_1}^{\alpha_1}\cdots\tau_{j_1}^{\alpha_m})\cdots(\tau_{j_L}^{\alpha_1}\cdots\tau_{j_L}^{\alpha_m})} \\
&= e^{\frac{1}{2^n}\left\{\sum_{m=0}^{n}\sum_{\langle\alpha_1,\cdots,\alpha_m\rangle}\sum_{\langle i_1,\cdots,i_K\rangle}\left(S_{i_1}^{\alpha_1}\cdots S_{i_1}^{\alpha_m}Z_{i_1}\right)\cdots\left(S_{i_K}^{\alpha_1}\cdots S_{i_K}^{\alpha_m}Z_{i_K}\right)\sum_{\langle j_1,\cdots,j_L\rangle}\left(\tau_{j_1}^{\alpha_1}\cdots\tau_{j_1}^{\alpha_m}Y_{j_1}\right)\cdots\left(\tau_{j_L}^{\alpha_1}\cdots\tau_{j_K}^{\alpha_m}Y_{j_L}\right)\right\}} \\
&\simeq e^{\frac{1}{2^n}\left\{\sum_{m=0}^{n}\sum_{\langle\alpha_1,\cdots,\alpha_m\rangle}\frac{1}{K!}\left(\sum_{i=1}^{N}S_i^{\alpha_1}\cdots S_i^{\alpha_m}Z_i\right)^K\frac{1}{L!}\left(\tau_j^{\alpha_1}\cdots\tau_j^{\alpha_m}Y_j\right)^L\right\}}.
\end{aligned} \tag{A17}$$

Using the identities

$$\begin{aligned}
1 &= \int dq_{\alpha_1,\cdots,\alpha_m}\delta\left(\sum_{i=1}^{N}S_i^{\alpha_1}\cdots S_i^{\alpha_m}Z_i - q_{\alpha_1,\cdots,\alpha_m}\right), \\
1 &= \int dr_{\alpha_1,\cdots,\alpha_m}\delta\left(\sum_{j=1}^{M}\tau_j^{\alpha_1}\cdots\tau_j^{\alpha_m}Y_j - r_{\alpha_1,\cdots,\alpha_m}\right)
\end{aligned} \tag{A18}$$

and going through the same steps as in Eqs. (A9 - A12), we arrive at

$$\prod_{\langle i_1,\cdots,i_K;j_1,\cdots,j_L\rangle}\left[1+(Z_{i_1}\cdots Z_{i_K}Y_{j_1}\cdots Y_{j_L})\prod_{\alpha=1}^{n}\frac{1}{2}\left(1+S_{i_1}^{\alpha}\cdots S_{i_K}^{\alpha}\tau_{j_1}^{\alpha}\cdots\tau_{j_L}^{\alpha}\right)\right]$$
$$=\prod_{m=0}^{n}\prod_{\langle\alpha_1,\cdots,\alpha_m\rangle}\int dq_{\alpha_1,\cdots,\alpha_m}\delta\left(\sum_{i=1}^{N}S_i^{\alpha_1}\cdots S_i^{\alpha_m}Z_i-q_{\alpha 1,\cdots,\alpha_m}\right)$$
$$\times\int dr_{\alpha_1,\cdots,\alpha_m}\delta\left(\sum_{j=1}^{M}\tau_j^{\alpha_1}\cdots\tau_j^{\alpha_m}Y_j-r_{\alpha 1,\cdots,\alpha_m}\right)\exp\left(\frac{1}{2^n}\left\{\sum_{m=0}^{n}\sum_{\langle\alpha_1,\cdots,\alpha_m\rangle}\frac{q^K_{\alpha_1,\cdots,\alpha_m}}{K!}\frac{r^L_{\alpha_1,\cdots,\alpha_m}}{L!}\right\}\right)$$
$$\simeq \mathrm{extr}_{\{\boldsymbol{q},\hat{\boldsymbol{q}},\boldsymbol{r},\hat{\boldsymbol{r}}\}}\left\{\exp\left[\frac{1}{2^n}\left\{\sum_{m=0}^{n}\sum_{\langle\alpha_1,\cdots,\alpha_m\rangle}\frac{q^K_{\alpha_1,\cdots,\alpha_m}}{K!}\frac{r^L_{\alpha_1,\cdots,\alpha_m}}{L!}\right\}\right.\right.$$
$$-\sum_{m=0}^{n}\sum_{\langle\alpha_1,\cdots,\alpha_m\rangle}q_{\alpha_1,\cdots,\alpha_m}\hat{q}_{\alpha_1,\cdots,\alpha_m}-\sum_{m=0}^{n}\sum_{\langle\alpha_1,\cdots,\alpha_m\rangle}r_{\alpha_1,\cdots,\alpha_m}\hat{r}_{\alpha_1,\cdots,\alpha_m}$$
$$\left.\left.+\sum_{m=0}^{n}\sum_{\langle\alpha_1,\cdots,\alpha_m\rangle}\hat{q}_{\alpha_1,\cdots,\alpha_m}\sum_{i=1}^{N}S_i^{\alpha_1}\cdots S_i^{\alpha_m}Z_i+\sum_{m=0}^{n}\sum_{\langle\alpha_1,\cdots,\alpha_m\rangle}\hat{r}_{\alpha_1,\cdots,\alpha_m}\sum_{j=1}^{M}\tau_j^{\alpha_1}\cdots\tau_j^{\alpha_m}Y_j\right]\right\}. \quad \text{(A19)}$$

In order to proceed further, one has to make an assumption about the order parameter symmetry. We adopt here the replica symmetric ansatz for the order parameters q, r, $\hat{q}$ and $\hat{r}$. This implies that the order parameters do not depend on the explicit indices but only on their number. It is therefore convenient to represent them as moments of random variables defined over the interval $[-1,1]$

$$q_{\alpha_1,\cdots,\alpha_l}=q\int dx\ \pi(x)\ x^l,\quad r_{\alpha_1,\cdots,\alpha_l}=r\int dy\ \rho(y)\ y^l,$$
$$\hat{q}_{\alpha_1,\cdots,\alpha_l}=\hat{q}\int d\hat{x}\ \hat{\pi}(\hat{x})\ \hat{x}^l,\quad \hat{r}_{\alpha_1,\cdots,\alpha_l}=\hat{r}\int d\hat{y}\ \hat{\rho}(\hat{y})\ \hat{y}^l, \quad \text{(A20)}$$

Then, each term in Eq.(A19) takes the form

$$\sum_{m=0}^{n}\sum_{\langle\alpha_1,\cdots,\alpha_m\rangle}\frac{q^K_{\alpha_1,\cdots,\alpha_m}}{K!}\frac{r^L_{\alpha_1,\cdots,\alpha_m}}{L!}=\frac{q^K}{K!}\frac{r^L}{L!}\sum_{m=0}^{n}\binom{n}{m}\int\prod_{k=1}^{K}dx_k\pi(x_k)x_k^m\int\prod_{l=1}^{L}dy_l\rho(y_l)y_l^m$$
$$=\frac{q^K}{K!}\frac{r^L}{L!}\int\prod_{k=1}^{K}dx_k\ \pi(x_k)\int\prod_{l=1}^{L}dy_l\ \rho(y_l)\left(1+\prod_{k=1}^{K}x_k\prod_{l=1}^{L}y_l\right)^n \quad \text{(A21)}$$
$$\sum_{m=0}^{n}\sum_{\langle\alpha_1,\cdots,\alpha_m\rangle}q_{\alpha_1,\cdots,\alpha_m}\hat{q}_{\alpha_1,\cdots,\alpha_m}=q\hat{q}\sum_{m=0}^{n}\binom{n}{m}\int dx\ d\hat{x}\ \pi(x)\ \hat{\pi}(\hat{x})x^m\ \hat{x}^m$$
$$=q\hat{q}\int dx\ d\hat{x}\ \pi(x)\ \hat{\pi}(\hat{x})\,(1+x\hat{x})^n \quad \text{(A22)}$$
$$\sum_{m=0}^{n}\sum_{\langle\alpha_1,\cdots,\alpha_m\rangle}\hat{q}_{\alpha_1,\cdots,\alpha_m}\sum_{i=1}^{N}S_i^{\alpha_1}\cdots S_i^{\alpha_m}Z_i=\hat{q}\sum_{i=1}^{N}Z_i\int d\hat{x}\ \hat{\pi}(\hat{x})\sum_{m=0}^{n}\hat{x}^m\sum_{\langle\alpha_1,\cdots,\alpha_m\rangle}S_i^{\alpha_1}\cdots S_i^{\alpha_m}$$

$$= \hat{q} \sum_{i=1}^{N} Z_i \int d\hat{x}\ \hat{\pi}(\hat{x}) \prod_{\alpha=1}^{n} (1 + S_i^\alpha \hat{x})\ . \tag{A23}$$

Substituting these into (A19), one obtains

$$\begin{aligned}
&\langle Z(\boldsymbol{\xi}, \boldsymbol{\zeta}, \mathcal{D})^n \rangle_{\boldsymbol{\xi},\boldsymbol{\zeta},\mathcal{D}} \\
&= \sum_{\boldsymbol{S}^1 \cdots \boldsymbol{S}^n} \sum_{\boldsymbol{\tau}^1 \cdots \boldsymbol{\tau}^n} \prod_{i=1}^{N} \left\langle \exp\left(\xi F_s \sum_{\alpha=1}^{n} S_i^\alpha \right) \right\rangle_\xi \times \prod_{j=1}^{M} \left\langle \exp\left(\zeta F_n \sum_{\alpha=1}^{n} \tau_j^\alpha \right) \right\rangle_\zeta \\
&\times \mathcal{N}^{-1} \prod_{i=1}^{N} \left\{ \oint \frac{dZ_i}{2\pi i} Z_i^{-(C+1)} \right\} \prod_{j=1}^{M} \left\{ \oint \frac{dY_j}{2\pi i} Y_j^{-(L+1)} \right\} \\
&\times \mathrm{extr}_{\{\pi,\hat{\pi},\rho,\hat{\rho}\}} \left\{ \exp\left[\frac{1}{2^n} \left\{ \frac{q^K}{K!} \frac{r^L}{L!} \int \prod_{l=1}^{K} dx_l\ \pi(x_l) \int \prod_{l=1}^{L} dy_l\ \rho(y_l) \left(1 + \prod_{l=1}^{K} x_l \prod_{l=1}^{L} y_l \right)^n \right\} \right.\right. \\
&- q\hat{q} \int dx\ d\hat{x}\ \pi(x)\ \hat{\pi}(\hat{x})(1 + x\hat{x})^n - r\hat{r} \int dy\ d\hat{y}\ \rho(y)\ \hat{\rho}(\hat{y})(1 + y\hat{y})^n \\
&\left.\left. + \hat{q} \sum_{i=1}^{N} Z_i \int d\hat{x}\ \hat{\pi}(\hat{x}) \prod_{\alpha=1}^{n} (1 + S_i^\alpha \hat{x}) + \hat{r} \sum_{j=1}^{M} Y_j \int d\hat{y}\ \hat{\rho}(\hat{y}) \prod_{\alpha=1}^{n} (1 + \tau_j^\alpha \hat{y}) \right] \right\}.
\end{aligned} \tag{A24}$$

The term involving the spin variables S is easily evaluated using the residue theorem

$$\begin{aligned}
&\sum_{\boldsymbol{S}^1 \cdots \boldsymbol{S}^n} \prod_{i=1}^{N} \left\langle \exp\left(\xi F_s \sum_{\alpha=1}^{n} S_i^\alpha \right) \right\rangle_\xi \prod_{i=1}^{N} \left\{ \oint \frac{dZ_i}{2\pi i} Z_i^{-(C+1)} \right\} \times \exp\left[\hat{q} \sum_{i=1}^{N} Z_i \int d\hat{x}\ \hat{\pi}(\hat{x}) \prod_{\alpha=1}^{n} (1 + S_i^\alpha \hat{x}) \right] \\
&= \left(\frac{\hat{q}^C}{C!} \int \prod_{l=1}^{C} d\hat{x}_l\ \hat{\pi}(\hat{x}_l) \left\langle \prod_{\alpha=1}^{n} \left\{ e^{\xi F_s} \prod_{l=1}^{C} (1 + \hat{x}_l) + e^{-\xi F_s} \prod_{l=1}^{C} (1 - \hat{x}_l) \right\} \right\rangle_\xi \right)^N,
\end{aligned} \tag{A25}$$

and similarly for the term involving the variables τ. Substituting these into Eq. (A24), one obtains the n-th moment of partition function

$$\begin{aligned}
&\langle \mathcal{Z}(\boldsymbol{\xi}, \boldsymbol{\zeta}, \mathcal{D})^n \rangle_{\xi,\zeta,\mathcal{D}} \\
&= \mathrm{extr}_{\{\pi,\hat{\pi},\rho,\hat{\rho}\}} \left\{ \exp\left[-NC \left\{ \int dx\ d\hat{x}\ \pi(x)\ \hat{\pi}(\hat{x}) \ln(1 + x\hat{x})^n - 1 \right\} \right.\right. \\
&- ML \left\{ \int dy\ d\hat{y}\ \rho(y)\ \hat{\rho}(\hat{y}) \ln(1 + y\hat{y})^n - 1 \right\} \\
&\left. + \frac{1}{2^n} \left\{ \frac{NC}{K} \int \left[\prod_{k=1}^{K} dx_k\ \pi(x_k) \right] \left[\prod_{l=1}^{L} dy_l \rho(y_l) \right] \ln\left[1 + \prod_{k=1}^{K} x_k \prod_{l=1}^{L} y_l \right]^n - 1 \right\} \right] \\
&\times \left(\int \left[\prod_{k=1}^{C} d\hat{x}_k \hat{\pi}(\hat{x}_k) \right] \left\langle \left(\left[e^{F_s \xi} \prod_{k=1}^{C} (1 + \hat{x}_k) + e^{-F_s \xi} \prod_{k=1}^{C} (1 - \hat{x}_k) \right] \right)^n \right\rangle_\xi \right)^N \\
&\times \left(\int \left[\prod_{l=1}^{L} d\hat{y}_l \hat{\rho}(\hat{y}_l) \right] \left\langle \left(\left[e^{F_n \zeta} \prod_{l=1}^{L} (1 + \hat{y}_l) + e^{-F_n \zeta} \prod_{l=1}^{L} (1 - \hat{y}_l) \right] \right)^n \right\rangle_\zeta \right)^M \Bigg\}.
\end{aligned} \tag{A26}$$

Finally, in the limit $n \to 0$ one obtains

$$\frac{1}{N}\langle \ln \mathcal{Z}(\boldsymbol{\xi},\boldsymbol{\zeta},\mathcal{D})\rangle_{\xi,\zeta,\mathcal{D}} = \lim_{n\to 0} \frac{\langle \mathcal{Z}(\boldsymbol{\xi},\boldsymbol{\zeta},\mathcal{D})^n\rangle_{\xi,\zeta,\mathcal{D}} - 1}{nN}$$
$$= \mathrm{extr}_{\{\pi,\hat{\pi},\rho,\hat{\rho}\}} \left\{ -\frac{C}{K}\ln 2 - C\int dx\ d\hat{x}\ \pi(x)\hat{\pi}\ (\hat{x})\ln(1+x\hat{x}) - \frac{CL}{K}\int dy\ d\hat{y}\ \rho(y)\ \hat{\rho}(\hat{y})\ln(1+y\hat{y}) \right.$$
$$+\frac{C}{K}\int \left[\prod_{k=1}^{K} dx_k \pi(x_k)\right]\left[\prod_{l=1}^{L} dy_l \rho(y_l)\right]\ln\left[1+\prod_{k=1}^{K} x_k \prod_{l=1}^{L} y_l\right]$$
$$+\int \left[\prod_{k=1}^{C} d\hat{x}_k \hat{\pi}(\hat{x}_k)\right]\left\langle \ln\left[e^{F_s\xi}\prod_{k=1}^{C}(1+\hat{x}_k) + e^{-F_s\xi}\prod_{k=1}^{C}(1-\hat{x}_k)\right]\right\rangle_{\xi}$$
$$\left. +\frac{C}{K}\int \left[\prod_{l=1}^{L} d\hat{y}_l \hat{\rho}(\hat{y}_l)\right]\left\langle \ln\left[e^{F_n\zeta}\prod_{l=1}^{L}(1+\hat{y}_l) + e^{-F_n\zeta}\prod_{l=1}^{L}(1-\hat{y}_l)\right]\right\rangle_{\zeta} \right\}. \tag{A27}$$

APPENDIX B: EVALUATION OF THE MAGNETISATION

Here, we derive explicitly Eqs.(18) and (19). After using the gauge transformation $S_i \to \xi_i S_i$, the magnetisation can be written as

$$m = \frac{1}{N}\sum_{i=1}^{N} \langle \mathrm{sign}(m_i)\rangle_{\boldsymbol{\xi},\boldsymbol{\zeta},\mathcal{D}}\ , \tag{B1}$$

introducing the notation $m_i = \langle S_i \rangle_{\beta\to\infty}$ (gauged average).

For an arbitrary natural number p, one can compute p-th moment of m_i

$$\langle {m_i}^p\rangle_{\boldsymbol{\xi},\boldsymbol{\zeta},\mathcal{D}} = \lim_{n\to 0}\lim_{\beta\to\infty}\left\langle \sum_{\{\boldsymbol{S}^1,\boldsymbol{\tau}^1\},\ldots,\{\boldsymbol{S}^n,\boldsymbol{\tau}^n\}} S_i^1\cdot S_i^2\cdot\ldots\cdot S_i^p e^{-\beta\sum_{a=1}^{n}\mathcal{H}_a}\right\rangle_{\boldsymbol{\xi},\zeta,\mathcal{D}}, \tag{B2}$$

where $\mathcal{H}_a$ denotes the gauged Hamiltonian of the a-th replica. Decoupling the dynamical variables and introducing auxiliary functions $\pi(\cdot)$, $\hat{\pi}(\cdot)$, $\rho(\cdot)$ and $\hat{\rho}(\cdot)$, of a similar form to Eq. (A20), one obtains

$$\langle {m_i}^p\rangle_{\boldsymbol{\xi},\boldsymbol{\zeta},\mathcal{D}} = \int \prod_{l=1}^{C} d\hat{x}_l\ \hat{\pi}(\hat{x}_l)\left\langle \tanh^p\left(F_s\xi + \sum_{k=1}^{C}\tanh^{-1}\hat{x}_k\right)\right\rangle_{\xi}, \tag{B3}$$

using the saddle point solution of $\hat{\pi}(\cdot)$.

Employing the identity

$$\mathrm{sign}(x) = -1 + 2\lim_{n\to\infty}\sum_{m=0}^{n}\binom{2n}{m}\left(\frac{1+x}{2}\right)^{2n-m}\left(\frac{1-x}{2}\right)^{m} \tag{B4}$$

which holds for any arbitrary real number $x \in [-1, 1]$ and Eqs.(B3) and (B4) one obtains

$$\begin{aligned}\langle \text{sign}(m_i) \rangle_{\boldsymbol{\xi},\boldsymbol{\zeta},\mathcal{D}} &= -1 + 2 \int dz\ \phi(z)\ \lim_{n\to\infty} \sum_{m=0}^{n} \binom{2n}{m} \left(\frac{1+z}{2}\right)^{2n-m} \left(\frac{1-z}{2}\right)^{m} \\ &= \int dz\ \phi(z)\ \text{sign}(z), \end{aligned} \tag{B5}$$

where we introduced a new notation for the distribution

$$\phi(z) = \int \prod_{l=1}^{C} d\hat{x}_l\ \hat{\pi}(\hat{x}_l) \left\langle \delta(z - F_s\xi - \sum_{k=1}^{C} \tanh^{-1} \hat{x}_k) \right\rangle_{\xi}, \tag{B6}$$

thus reproducing Eqs.(18) and (19).

REFERENCES

[1] C.E. Shannon, *Bell Sys.Tech.J.*, **27**, 379 (1948); **27**, 623 (1948).

[2] R.G. Gallager, *IRE Trans.Info.Theory,* **IT-8,** 21 (1962).

[3] D.J.C. MacKay and R.M. Neal, *Elect. Lett.*, **33**, 457 (1997);D.J.C. MacKay, *IEEE Trans.IT*, **45**, 399 (1999).

[4] I. Kanter and D. Saad, *Phys.Rev.Lett.* **83**, 2660 (1999); *Jour. Phys. A* **33**, 1675 (2000).

[5] M.G. Luby, M. Mitzenmacher, M.A. Shokrollabi and D.A.Spielman, *in Proceedings. of the IEEE International Symposium on Information Theory (ISIT)*, 117 (1998).

[6] D.J.C. MacKay, S.T. Wilson and M.C. Davey, *IEEE Trans.Comm.*, **47**, 1449 (1999).

[7] T. Richardson, A. Shokrollahi and R. Urbanke, *Design of Provably Good Low-Density Parity Check Codes,* http://cm.bell-labs.com/cm/ms/who/tjr/pub.html (1999)

[8] Y. Kabashima and D. Saad, *Europhys.Lett.,* **44**, 668 (1998).

[9] Y. Kabashima and D. Saad, *Europhys.Lett.,* **45** 97 (1999).

[10] Y. Kabashima, T. Murayama and D. Saad, *Phys. Rev. Lett.,* **84**, 1355 (2000); Y. Kabashima, T. Murayama, R. Vicente and D. Saad, *Advances in Neural Information Processing Systems 12* (MIT press) 272 (2000).

[11] R. Vicente, D. Saad and Y. Kabashima, *Phys. Rev. E,* **60** 5352 (1999).

[12] B.J. Frey, *Graphical Models for Machine Learning and Digital Communication* (MIT Press), (1998).

[13] J.Pearl, *Probabilistic Reasoning in Intelligent Systems: Networks of Plausible Inference* (Morgan Kaufmann), (1988).

[14] D. Thouless, P.W. Anderson and R.G. Palmer, *Phil. Mag.*, **35**, 593 (1977).

[15] N. Sourlas, *Nature*, **339**, 693 (1989).

[16] Y. Iba, *J. Phys. A,* **32**, 3875 (1999).

[17] H. Nishimori, *J. Phys. Soc. Jpn.*, **62**, 2793 (1993).

[18] P. Rujan, *Phys. Rev. Lett.*, **70**, 2968 (1993).

[19] N. Sourlas, *Europhys.Lett.*, **25**, 159 (1994).

[20] K.Y.M. Wong and D. Sherrington, *J.Phys.A*, **20**, L793 (1987);

[21] H. Nishimori, *Prog.Theo.Phys.*, **66**, 1169 (1981).

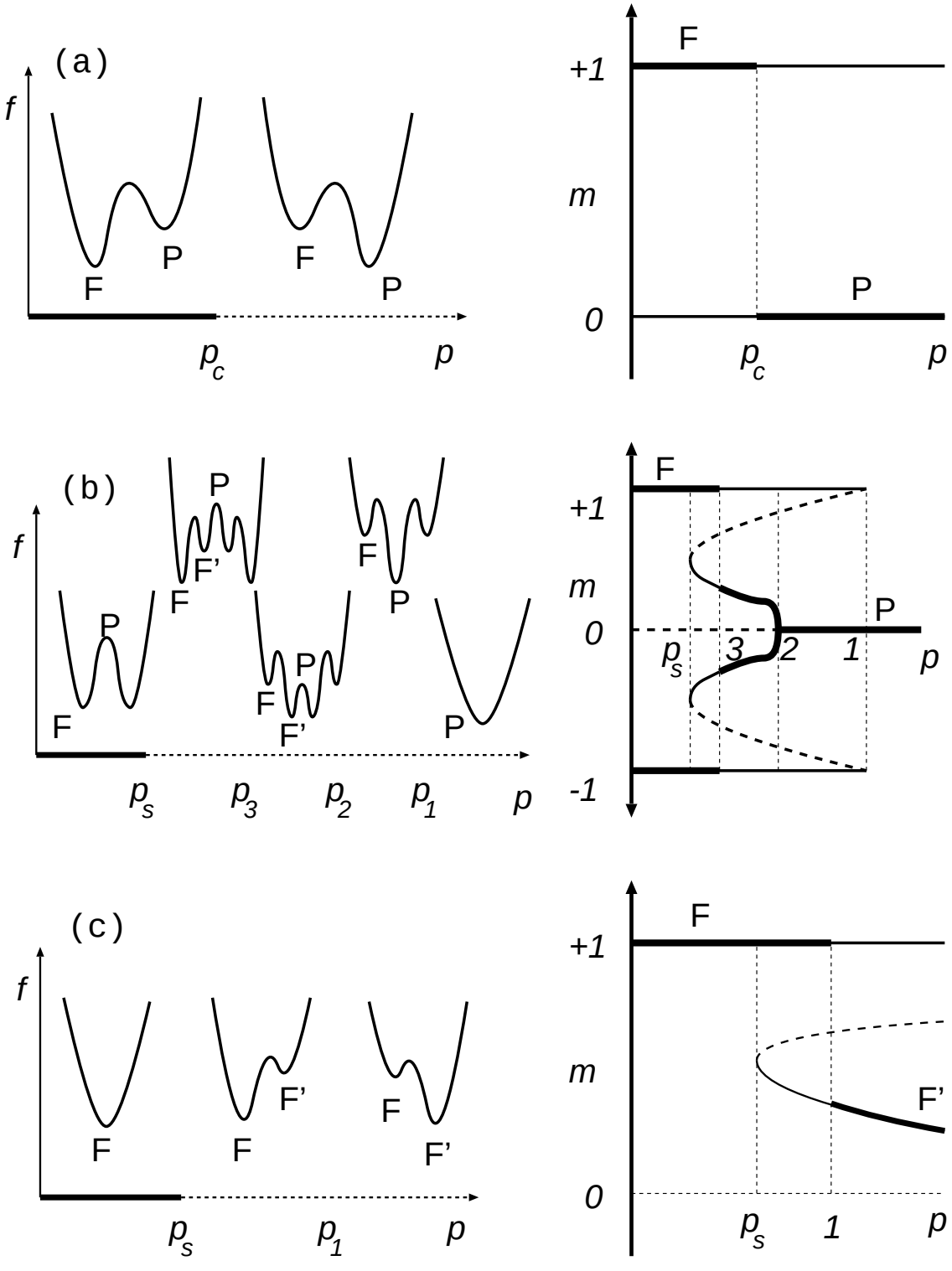
(a)
f
F
P
F
P
p_c
p
F
+1
m
0
P
p_c
p
(b)
f
P
F'
F
F
P
P
F
P
F
F'
P
p_s
p_3
p_2
p_1
p
F
+1
m
0
P
p_s
3
2
1
p
-1
(c)
f
F
F'
F
F
F'
p_s
p_1
p
F
+1
m
F'
0
p_s
1
p

FIG. 1. Left hand figures show a schematic representation of the free energy landscape while figures on the right show the ferromagnetic, sub-optimal ferromagnetic and paramagnetic solutions as functions of the noise rate p; thick and thin lines denote stable solutions of lower and higher free energies respectively, dashed lines correspond to unstable solutions. (a) $K \geq 3$ or $L \geq 3$, $K > 1$; the solid line in the horizontal axis represents the phase where the ferromagnetic solution (F, $m = 1$) is thermodynamically dominant, while the paramagnetic solution (P, $m = 0$) becomes dominant for the other phase (dashed line). The critical noise p_c denotes Shannon's channel capacity. (b) $K = 2$ and $L = 2$; the ferromagnetic solution and its mirror image are the only minima of the free energy over a relatively small noise level (the solid line in the horizontal). The critical point,due to dynamical considerations, is the spinodal point p_s where sub-optimal ferromagnetic solutions (F', $m < 1$) emerge. The thermodynamic transition point p_3, at which the ferromagnetic solution loses its dominance, is below the maximum noise level given by the channel capacity, which implies that these codes do not saturate Shannon's bound even if optimally decoded. (c) $K = 1$; the solid line in the horizontal axis represents the range of noise levels where the ferromagnetic state (F) is the only minimum of the free energy. The sub-optimal ferromagnetic state (F') appears in the region represented by the dashed line. The spinodal point p_s, where F' solution first appears, provides the highest noise value in which convergence to the ferromagnetic solution is guaranteed. For higher noise levels, the system becomes bistable and an additional unstable solution for the saddle point equations necessarily appears. A thermodynamical transition occurs at the noise level p_1 where the state F' becomes dominant.

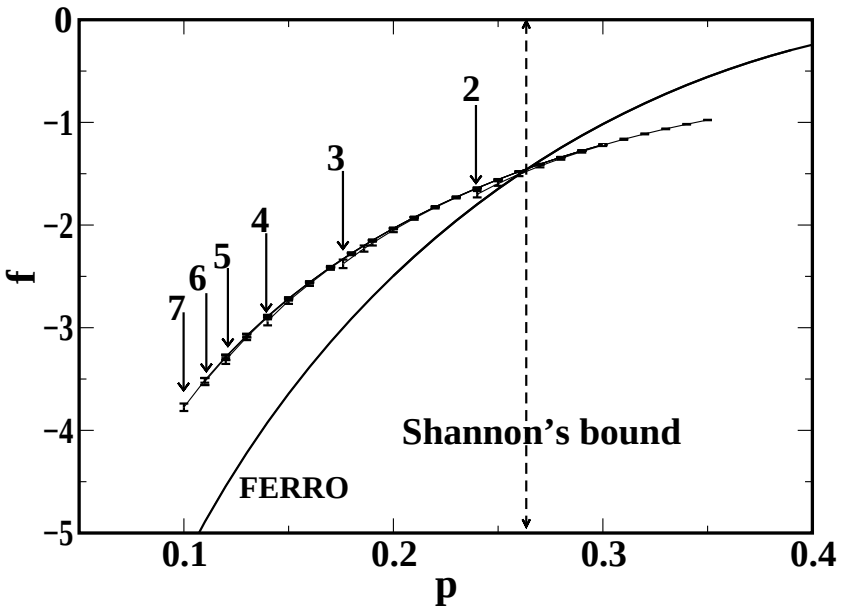

FIG. 2. Free energies obtained by solving the analytical equations using Monte-Carlo integrations for $K = 1$, $R = 1/6$ and several values of L. Full lines represent the ferromagnetic free energy (FERRO, higher on the right) and the suboptimal ferromagnetic free energy (higher on the left) for values of $L = 1, ..., 7$. The dashed line indicates Shannon's bound and the arrows represent the spinodal point values p_s for $L = 2, ..., 7$. The thermodynamic transition is very close, but bellow, the channel capacity ($p_1 \approx 0.261$ against $p_c \approx 0.264$ at $R = 1/6$).

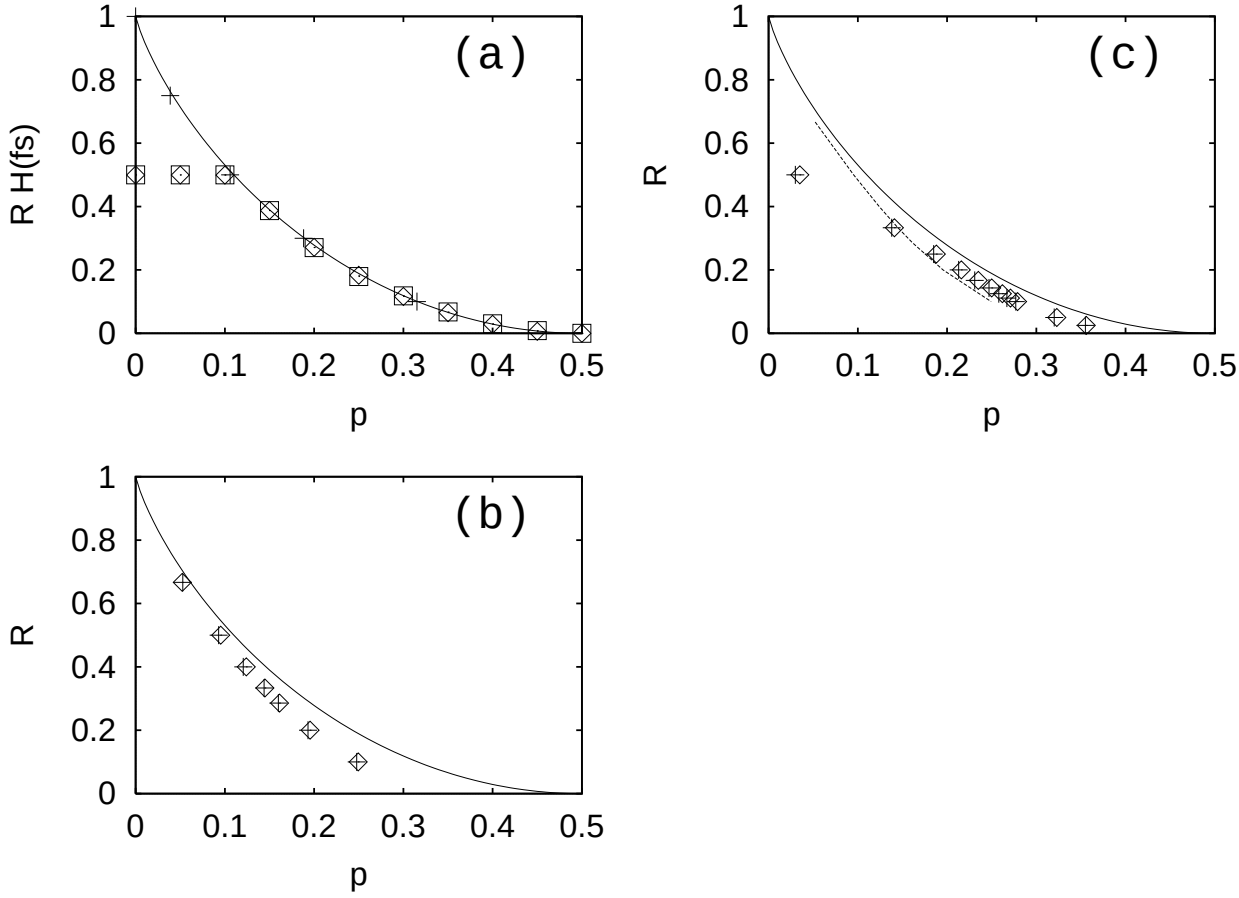

FIG. 3. Critical code rate as a function of the flip rate p, obtained from numerical solutions and the TAP approach ($N=10^4$), and averaged over 10 different initial conditions with error bars much smaller than the symbols size. (a) Numerical solutions for $K=L=3$, $C=6$ and varying input bias f_s ($\Box$) and TAP solutions for both unbiased ($+$) and biased ($\diamond$) messages; initial conditions were chosen close to the analytical ones. The critical rate is multiplied by the source information content to obtain the maximal information transmission rate, which clearly does not go beyond $R=3/6$ in the case of biased messages; for unbiased patterns $H_2(f_s)=1$. (b) For the unbiased case of $K=L=2$; initial conditions for the TAP ($+$) and the numerical solutions ($\diamond$) were chosen to be of almost zero magnetisation. (c) For the case of $K=1$, $L=2$ and unbiased messages. We show numerical solutions of the analytical equations ($\diamond$) and those obtained by the TAP approach ($+$). The dashed line indicates the performance of $K=L=2$ codes for comparison. Codes with $K=1$, $L=2$ outperform $K=L=2$ for code rates $R<1/3$.

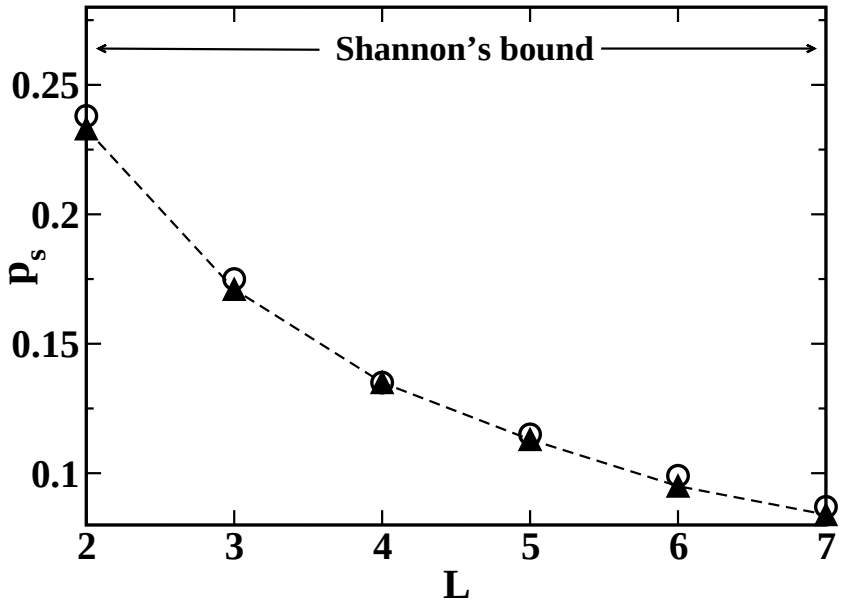

FIG. 4. The spinodal point noise level p_s for $K = 1$, $R = 1/6$ and several choices of L. Numerical solutions are denoted by circles and TAP decoding solutions ($N = 10^4$) by black triangles.

TABLES

TABLE I. Comparison between the maximal tolerable noise level for codes based on randomly and systematically structured matrices in the case of $K = L = 2$; decoding is carried out using BP/TAP and the transmission channel used is the BSC. The performance of both matrix structures is highly similar.

Rate $R = K/C$	0.6666	0.5	0.4	0.3333	0.2857	0.2	0.1
Systematic Matrix	0.0527	0.0934	0.1222	0.1416	0.1598	0.1927	0.2476
	$\pm$0.0016	$\pm$0.0019	$\pm$0.0012	$\pm$0.0016	$\pm$0.0007	$\pm$0.0016	$\pm$0.0010
Random Matrix	0.0528	0.0930	0.1206	0.1439	0.1599	0.1931	0.2477
	$\pm$0.0009	$\pm$0.0019	$\pm$0.0010	$\pm$0.0017	$\pm$0.0010	$\pm$0.0014	$\pm$0.0014